SSRO

Single Source
Regulations Office

SSRO-C-127 Digital Board Software

Appendix 1: Specification

1. Introduction

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

1.2 When undertaking its statutory functions, the SSRO aims 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 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 Services

Service overview

2.1 The SSRO requires Digital Board Software that will allow administrators to upload meeting packs and documents for access by meeting participants at any location. Participants must be able to annotate and comment on papers and to access their papers and notes whether online or offline.

2.2 Under current arrangements, there are around 26 users of the SSRO's Software including three administrators, who manage and upload content. Different levels of user rights are necessary, including limiting access to particular committees, reading rooms/libraries and individual documents. We require the number of users to be extended to 35.

2.3 The SSRO envisages using the system for all the SSRO's formal groups, including for all Board, sub-committees (currently four) and Senior Leadership meetings. There are around 30 regular meetings per year.

2.4 The services that the SSRO requires are summarised in the table below and set out in full in this Specification, including the Key Performance indicators (KPI's) in Annex 1.

Required service	Service overview
Administrator requirements	Provision of software that can create agendas, compile and publish papers from templates.
Meeting participant requirements	Provision of a user-friendly interface for meeting participants, with simple navigation between papers on the agenda for up to 35 users (including 3 administrators).
Non-functional requirements	A service that is supported on a variety of platforms, and a customer support team that is available and quick to respond remotely to all users of the software. Secure storage and management of the SSRO's data, which complies with the prescribed security requirements

3. Core system and software service requirements

3.1 The SSRO requires the provision of a Digital Board Software package, the development and administration of the system, end user training and ongoing support for up to 35 users, including three administrators. The SSRO may also require, from time to time, provision for temporary additional users. The number of additional temporary users per year is unlikely to exceed five.

3.2 The SSRO also requires the management of the SSRO's data, ensuring that it is kept safe, secure and available. Much of the information uploaded onto the system will be highly sensitive, including information to which Schedule 5 of the Defence Reform Act 2014 applies. Unauthorised disclosure of such information is a criminal offence.

3.3 The SSRO's core requirements are set out below and are in three areas: requirements for administrators; requirements for meeting participants; and additional requirements, which are desirable. Where the Supplier has committed to providing any of the Additional requirements identified in the Specification, the Supplier shall be contractually required to deliver them. The KPI's which the Supplier is required to achieve are outlined in Annex 1 to this document.

Deliverables

3.4 For **Administrators**, the Digital Board Software will:

a) Create agendas, compile and publish papers intuitively from a template, with a drag and drop facility.

b) Provide the ability to upload documents in their native format, with no need to convert to PDF before upload, and a faithful conversion of any file format.

c) Provide the ability for the administrator to set detailed user permissions that allow control over access to meetings and individual documents.

d) Distribute packs of papers instantly to participants, with email alerts sent directly from the system.

e) Allow simple, instant republishing of individual papers in a pack, while retaining annotations that have already been made by meeting participants on previous versions of that paper.

f) Provide the ability for the administrator to download the final pack of Board papers into a single PDF.

g) Provide the ability to manage licenses and user passwords from within the system without the need to contact the Supplier.

h) Provide for multiple committee areas to be set up and managed. Users must only have access to specified committee areas, as set by the administrator.

i) Provide the ability to set up a library/reading room area to store static documents and supplementary documents relating to a specific committee.

j) Be able to integrate with common platforms such as Microsoft Teams, Outlook and SharePoint with the ability to join meetings from within the system.

k) Allow the functionality of links to external web addresses within uploaded documents and the ability to link to documents stored in the library/reading rooms.

3.5 For **meeting participants/users**, the software will:

a) Be easy to use, with an intuitive interface and simple navigation between papers on the agenda. Meeting packs should include automatic page numbers, links and navigation tools such as tabs for individual papers.

b) Allow meeting participants to read, annotate, add notes and highlight electronically.

c) Provide an option to share annotations and notes with other meeting participants or mark annotations as private.

d) Allow meeting participants to work offline or online, with synchronisation of any changes that have occurred during the offline period.

e) Ensure that past meeting documents (starting from the service commencement date) are easily accessible within the software.

f) Provide a search function across meeting packs and documents stored on the system.

Additional deliverables

3.6 The following additional features are desirable:

a) Ability to print papers and annotations if required.

b) Functionality to record and assign actions within the system.

c) The ability to send users messages from within the system.

d) Reporting for administrators on user activity.

e) The ability to set approved devices from within the system.

f) Customisable dashboard.

Where the Supplier has committed to providing any Additional requirements, the Supplier shall be contractually required to deliver them.

Relationship

3.7 The Supplier must nominate a dedicated account manager whose role is to:

- manage the service and relationship between the Supplier and the SSRO on a day-to-day basis throughout the contract period;
- provide a primary point of contact for the SSRO throughout the contract period;
- ensure that the agreed KPIs (Annex 1) are met;
- ensure compliance with security requirements;
- remain consistently informed about the Supplier's performance on all matters;
- ensure support is available to address issues in a timely manner and meet any urgent requirements within an acceptable timeframe;
- ensure that the agreed fixed 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.

4. SSRO ICT and Security Requirements

4.1 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. This includes information to which Schedule 5 of the Defense Reform Act 2014 applies, unauthorised disclosure of which is a criminal offence.
- **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.

Deliverables

4.2 The SSRO takes the security of the information it holds very seriously, and the Supplier must at all times comply with the Security Conditions contained in Schedule 1 of the contract, and the Security Measures contained in Schedule 2 of the contract.

4.3 The SSRO IT environment, policies and procedures are based on the following policies and procedures and the system(s) provided by the Supplier for SSRO staff use must operate in this environment:

a) HMG Security Policy Framework (SPF).

b) NCSC Published Guidance, Cloud Security Principles and Security Design Principles.

c) ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

d) ISO/IEC 22301:2012 – Societal Security – Business Continuity Management Systems – Requirements.

e) Cyber Essentials Scheme: Requirement for Technical Protection from Cyber Attacks.

4.4 The Supplier (and any Sub-Contractors who will process SSRO Sensitive Information) must hold relevant and current ISO27001:2013 (or equivalent) accreditation certification and maintain this for the entire Contract Period.

4.5 The SSRO maintains Cyber Essentials Plus certification. Where the Supplier (and Sub-Contractors who will process SSRO Sensitive Information) holds Cyber Essentials Plus accreditation at the Commencement Date, such accreditation must be maintained by those parties for the entire Contract Period. Where the Supplier (or Sub-Contractors who will process SSRO Sensitive Information) do not hold Cyber Essentials Plus accreditation at the Commencement Date, such accreditation must be obtained within six months of the Commencement Date and maintained for the remainder of the Contract Period. A failure to comply with this requirement may result in termination of the contract.

4.6 The SSRO's IT environment uses the Microsoft platform including Windows 10, Office 365, Microsoft Entra ID (previously named Azure AD), Intune Endpoint Management and Enterprise Mobility and Security. When in the office SSRO staff connect to the internet via GovWifi provided by the Government Property Agency. SSRO Staff work regularly and frequently away from the office. Secure connectivity, within the office and when working remotely, is provided through a Zero Trust Architecture solution that utilises iBoss (**https://www.iboss.com**/). The Supplier must ensure that full system functionality is available to different SSRO user groups when connected to the office network and when working remotely. The SSRO's Secure Operations Centre (SOC) is currently provided by e2e assure (see **https://e2e-assure.com/soc-services/cyber-threat-detection/**).

4.7 Other participants access meeting papers and additional information using SSRO issued devices connecting via password secured Wi-Fi. Currently these are a mixture of iPad Pro 2 64GB 10.5-inch and iPad Pro 3 64GB 11-inch. These devices are registered and managed by Microsoft Intune Endpoint Management. The devices use fingerprint authentication.

4.8 Supplier staff who could access SSRO information in the system (e.g. privileged access technical staff) must have undergone the requirements of **HMG Baseline Personnel Security Standard (BPSS)**.

4.9 The Supplier must be able to disable user accounts 24/7 in the event of credential or device loss and wipe locally stored content remotely.

4.10 Any data export functionality such as downloading, emailing or printing must be optional so that these can be disabled or enabled by administrators (not by standard users).

Additional deliverables

4.11 The following additional features are desirable:

a) User authentication should be as easy as possible. A single sign on solution is desirable, and, in the case that this cannot be provided by the Supplier in the context of the SSRO environment specified above, multi factor authentication for all users must be implemented, managed, and maintained by the Supplier.

5. Set up and Transition Services

5.1 The set up and transition period shall commence upon entering into the contract, estimated to be 24 January 2024. The Supplier is required to plan the transition and undertake any necessary transition activities in good time for the new digital board service to commence on 5 March 2024 (the Service Commencement Date).

5.2 The Supplier shall work with the incumbent supplier (Decision Time) and the SSRO during the transition period to ensure that, at the Service Commencement Date, set up and transition is completed and that the Services are provided fully in accordance with this Specification and to the SSRO's reasonable satisfaction from that date.

5.3 The Supplier shall deploy the technology solution (including installation, where applicable) in preparation for securely transferring the historic data for the past 2 years, from the current system, in accordance with the ICT and Security conditions described in section 4 above.

5.4 Transition is deemed to have been completed and accepted, subject to other relevant terms of the Contract, only when the SSRO is satisfied that: a) data from incumbent systems has been transferred across and agreed by the SSRO as complete; b) the functionalities are tested and operable; c) the system meets with SSRO security requirements; d) training of SSRO staff is complete; e) the SSRO has access to the system from its designated offices

and from SSRO devices in remote locations; and f) the SSRO has no material concerns about the Supplier's ability to deliver the Services in accordance with the Contract.

5.5 There may be a need for parallel running of the service during the set up and transition period and to ensure data accuracy.

6. Training and Ongoing Support

Deliverables

6.1 The Supplier shall train up to four administrators from the SSRO on the functionalities and use of their technology/software platform, prior to the Service Commencement Date. The Contractor shall also provide a single training event for meeting participants/users.

6.2 The Supplier shall provide ongoing training as reasonably required to ensure a smooth running of the service and to foster greater understanding and ensure service delivery.

6.3 The Supplier shall ensure that a service team is available and prompt in responding remotely within office hours, both to administrators and meeting participants/users.

Additional deliverables

6.4 The following additional features are desirable:

a) A 24-hour support service team available and quick to respond remotely, both to administrators and meeting participants/users.

Annex 1: Key Performance Indicators

Part 1: Service Standards

1. The Supplier shall be available to provide support during the following hours of operation.

Monday	9.00am	5.30pm
Tuesday	9.00am	5.30pm
Wednesday	9.00am	5.30pm
Thursday	9.00am	5.30pm
Friday	9.00am	5.30pm
Saturday	Closed	Closed
Sunday	Closed	Closed
Bank Holidays	Closed	Closed

2. In order to ensure that a quality service is delivered, the Supplier shall achieve the following service standards.

Service Support and Uptime	Requirement
Telephone Support	Within 30 minutes of original call
Service Response/Resolution Time	Priority within 3 working hours Non-Priority within 6 working hours
Communication of planned downtime	5 working days
Initial communication of any other downtime	Within 2 hours
Uptime Guarantee	98%
First time fix	98%
Major incident recovery time (time to restore service)	24 hours

Part 2: System performance summary

1. System maintenance

1.1. The Supplier will ensure that the system/software(s) are maintained in line with the manufacturer's instructions and will include quality assurance checks and a service programme agreed and set out in the contract.

1.2. At no additional cost, planned servicing will take place at a frequency set out and agreed by the SSRO and the Supplier or more frequently if deemed necessary by the Supplier.

2. Uptime guarantee

2.1. The Supplier undertakes that throughout the Contract Period, the system(s) will achieve 98% full use by the SSRO at its site and remotely ("Uptime") and service levels (systems and back up) will exceed 98%, measured on a 12 hours per day, 5 days per week basis over fixed three month periods beginning on the Service Commencement Date (herein a "Quarterly Period"). A system will be considered to be not available if:

- it is unable to properly perform its core functions because of a network malfunction;
- the system/software is not producing correct results; or
- the software provided by the Supplier which supports the service are not fully operational to a level which would support full and proper use by the SSRO for any reason, providing it is the fault of the Supplier.

3. Downtime

3.1. "Downtime" shall mean time when the system/software(s) is not available in accordance with section 2.1 above, but shall not include periods of time during which a system/software(s) is unavailable for use as a consequence of:

- planned maintenance to the system which is actually performed;
- breakdown as a result of poor usage of the system/software by the SSRO;
- abuse, wilful damage or neglect on the SSRO's part;
- inaccessibility of the system/software to the Supplier or its representative at times when the SSRO had agreed to make this available for access; or
- failure of the system/software due to any event of Force Majeure.

3.2. Hours of Downtime shall be defined as the period during which the system/software(s) fails to function in accordance with the Contract in a substantial way. For the purpose of this, if the system/software fails to function, but those services can still be carried out (offline) without materially adversely affecting the operation of the SSRO, such failure shall not be considered downtime.

4. Business continuity and Disaster Recovery

4.1. In the event of a major incident, the Recovery Time Objective (time to restore service) should be no more than 24 hours. The Recovery Point Objective (potential data loss) should be no more than 8 hours. Downtime shall commence at the time when a call is placed by the SSRO to the Supplier requiring assistance. Downtime ends at the time at which the affected part or parts of the system/software(s) is again available for their applicable use under this Agreement. A log shall be kept and the time of all service calls to the Supplier shall be logged together with a joint entry of the SSRO and the Supplier's engineers/helpdesk detailing the end of the downtime period.

5. Service monitoring

5.1. The Supplier will appoint an Account Manager for the SSRO. The Account Manager shall ensure service levels are maintained and coordinate with SSRO staff regarding any Downtime.

5.2. Downtime will be calculated cumulatively over a Quarterly Period. Downtime in a Quarterly Period shall be calculated by reference to the average downtime across all systems in the SSRO's site, provided that the Supplier shall ensure that Uptime shall not fall below the required level of 98%.

5.3. Uptime and Downtime shall be measured quarterly but reported monthly by the SSRO to the Supplier.

5.4. The SSRO will monitor Uptime and Downtime with quarterly performance review logged and forwarded (emailed) to the Supplier.