Request for Proposal (RFP) for
Cybersecurity Testing Services for SEDRI LIMS

1. RFP Background

Wellcome Trust, in collaboration with Arcta Solutions Limited is seeking proposals from qualified cybersecurity firms to conduct comprehensive security testing of our Laboratory Information Management System SEDRI-LIMS. The goal is to identify potential vulnerabilities and provide guidance on any risk mitigations, to ensure the integrity, confidentiality, and availability of our digital product.

SEDRI-LIMS is a Laboratory Information Management system (LIMS), that is critical for managing patient data, test results, and ensuring seamless operations across the various functions, departments, and roles, that make up the laboratory workflow. Given the sensitive nature of the information processed, it is imperative that the system is secure against potential cyber threats and from unauthorised access, either accidental or forced, from both internal and external actors.

SEDRI-LIMS can be deployed in two ways:

i. Local Product Install: SEDRI-LIMS consists of open-source code that can be installed on a server connected to a laboratory's LAN (client server) or installed as a standalone instance (single device) running on a PC, located within a Laboratory environment and optionally connected to the laboratory's LAN. Installations are expected to be supported by Arcta Solutions Limited (the developer), but in theory can also be deployed unassisted, using installation guidelines. The resultant service is operated by the health care provider.
ii. SEDRI LIMS as a Service: SEDRI-LIMS can also be provided as a cloud-hosted service, with multi-factor-authentication as an additional security measure.

Both the 'product' and the 'service' are intended to be used by trained clinical staff and laboratory technicians, working as part of a Ministry of Health, or similar health care provider. While the product and service are primarily intended for use in Low-and-Middle-Income-Countries (LMICs), specifically in resource limited settings, target clients may include high income settings.

The vendor is invited to propose an approach to assuring the information security of SEDRI-LIMS. There are key objectives that this work should seek to achieve.

i. Ensure that the software is secure in that it does not allow anyone to access data they should not see or carry out functions in the system that they should not have access to.
ii. Ensure that any processes or procedures that are put in place to manage security are kept up to date with each new release of the system.
iii. Ensure that management of client data in the cloud by Arcta Solutions is done in accordance with best industry practices.
iv. SEDRI-LIMS interprets breakpoints using the CLSI and EUCAST standards and therefore may be considered to be a medical instrument. This may require the product and/or Arcta Solutions Limited to adopt specialist certifications. These must be identified as part of this work.

2. Contract Deliverables

The breakdown of costs for the project should be split into sections. It is possible that we may decide to stage the contract carrying out the higher priority sections first so make sure the cost for each section covers the complete cost of the work required. Outline separately if there are cost savings that can be made if two sections are carried out together so as not to

repeat work. The costs will be split into two major sections: Local Deployment and Cloud Deployment and then itemised to correspond to the seven subsections outlined below.

The total number of working days on this project will not be expected to exceed 55, to be distributed across the 6 months of the project.

		Local Deployment	***Cloud Deployment***
i.	**Strategy for achieving necessary certifications** Document(s) outlining which certifications(s) we should be pursuing for the product and why. Must also include a detailed plan outlining how the certification(s) will be achieved, including timescales.		
ii.	**Strategy for carrying out security testing** Document(s) describing how security testing will be carried out, this will include: – Detailed descriptions of the testing that needs to be carried out – Tools to be used – Who will be responsible for carrying out the testing – Any implications for security of publishing the code as open source		
iii.	**Strategy for handling personal data** Document containing policies and procedures to adopt for handling personal data and any changes that should be made to the system to handle this securely to meet accepted best practices and standards.		
iv.	**Process for incorporating security testing into our release pipeline** It is important that security for the system is maintained for each new release of the system including any urgent bug fix releases that are distributed for individual client installations. This deliverable includes the documentation and development of the ongoing processes which incorporate security testing into our release pipeline. If these processes include the use of any external agencies then the costs must be outlined.		
v.	**Carrying out security testing for the current release**		

		Local Deployment	*Cloud Deployment*
	The current release of the system must undergo security testing as outlined in the previous deliverables.		
vi.	**Development of and policies and procedures that must be followed by Arcta Solutions Limited** The current release of the system must undergo security testing as outlined in the previous deliverables.		
vii.	**Achievement of certifications** Obtaining the necessary certifications agreed as part of the certification strategy.		

Data Security

SEDRI-LIMS contains personal information and must be managed and secured in accordance with accepted standards of data management and privacy.

For local installations, it will be the client's responsibility to secure their data. However, for Cloud installations Arcta Solutions will manage the databases containing client information and will need to take full responsibility for securing this data in accordance with accepted standards.

SEDRI-LIMS has a client portal that allows external users to access segments of the personal data being used within the system over the internet. Users must not see other personal information held on the system that they should not have access to.

Technical Overview

SEDRI-LIMS uses a Postgresql database which is accessed through a .NET Framework 8 service layer.

Users access the system using a client hosted in a web browser. This client is written in Javascript and uses the REACT framework and FluentUI component framework.
Cloud instances of the system are hosted in Microsoft Azure.

For local installs forms based authentication is used. For cloud installs the Microsoft multifactor authentication available on Azure is used.

3. RFP Timetable

#	Activity	Responsibility	Date
1	RFP issued to Suppliers via website	Wellcome	20 November 2024
4	Submission of RFP Response	Supplier	7 January 2025
5	RFP Evaluation Period	Wellcome	8 January -16 January 2025
6	Supplier Interviews	Wellcome & Supplier	20 January – 31 January 2025
7	Notification of Contract Award	Wellcome	3 February 2025
8	Contract Negotiation	Wellcome & Supplier	February 2025
9	Contract Start Date	Wellcome & Supplier	March 2025

4. Response Format

The following headers support the timetable by providing further detail of the key steps.

RFP Questions

Suppliers submitting a full proposal should cover the following areas in their response:

#	Question	Max Pages
1	**Methodology:** Provide a short proposal outlining how you would approach the work and the proposed methodology (e.g. conducting the security assessments, including desired system setup and hosting). Please include communication plan with the Wellcome Team.	2
	Arcta Solutions: *As SEDRI-LIMS will be deployed worldwide, it is important that any customers of the system are assured that Arcta Solutions Limited have a strong and ongoing commitment to cyber security. To help us achieve this, please advise on any relevant internationally recognised certifications and how to obtain them in your methodology.* *Expected input and dependencies on Arcta Solutions to facilitate the testing.*	1

#	Question	Max Pages
2	**Experience:** What makes you best placed to fulfil the requirements outlined in this RFP? This could include networks and previous experience. Please feel free to include any relevant case studies. *Any CVs must be anonymised.*	2
3	**Delivery Plan:** Provide a proposed delivery plan outlining the project deliverables and timelines.	2
4	**Risk**: Outline any major risks and challenges you foresee with meeting Wellcome's requirements. Please include your mitigation strategies for these risk and challenges.	1
5	**Budget:** Provide a detailed budget including breakdown justifying the proposed costs as outlined in **2. Contract Deliverables** to meet Wellcome's requirements for both Local deployment and Cloud deployment.	Table
6	**EDI:** Outline your approach to equity, diversity, and inclusion (EDI) both in relation to your proposed methodology for the project, and within your team. For more information on EDI, see: https://www.inclusionhub.com/articles/what-is-dei	1
7	**Accessibility:** *All our content should be WCAG 2.2. AAA compliant. Any documents being provided to Wellcome must pass accessibility requirements. If you are unable to produce accessible documents, budget must be set aside to employ a suitable agency to do this work.*	N/A please confirm

Contract Feedback

This section allows Suppliers to provide specific feedback to the contractual agreement which will be used should their proposal be successful. This is the suppliers' opportunity to provide negotiation points on Wellcome's terms and conditions.

We will not consider negotiations that are raised in your response to this proposal I.e. after the contract has been awarded so as not to delay the contracting process. Please ensure you engage with a relevant legal contact if applicable. Contract feedback is to be incorporated into your proposal as an annex and in the following format;

Clause #	Issue	Proposed Solution/Comment

Suppliers submitting proposals as a registered company should review Wellcome's Standard terms and Conditions document.

Individuals submitting proposals as a sole trader (not registered) should notify RFP@wellcome.org

Individuals submitting proposals through their own personal services company please highlight this to the Wellcome contact immediately (see point 7 below).

Information Governance

Wellcome is committed to upholding data protection principles and protecting your information. The Wellcome-Privacy-Statement-2023.pdf explains how, and on what legal basis, we collect, store, and use personal information about you. This includes any information you provide in relation to this proposal.

Under GDPR/Data Protection law, Wellcome must keep a record of all personal information it is processing (i.e., collecting, using, and sharing). This record will be made available to the Information Commissioner's Office upon request.

This is Wellcome's record of data processing activities which meets GDPR article 30 requirements.

Suppliers will be asked to complete the TPSRA2 assessment before presentation stage to assess how you handle data.

5. Evaluation Criteria

During the RFP evaluation period the evaluation panel will independently evaluate your proposal against the criteria outlined below. All scores will be collated, discussed and a decision will be agreed on who progresses to the next stage of the procurement exercise.

Please note the evaluation panel will include representatives from Wellcome and Arcta.

Criteria	Details	%score
Methodology	*Detailed methodology for conducting the security assessments, including desired system setup and hosting.* *Coverage:* How well are the desired focus areas (as outlined in the specification) covered in the proposed methodology address? *Quality*: Is the proposed methodology aligned with our needs? *Utility*: Will the proposed methodology deliver the desired, credible, and useful results? *As SEDRI-LIMS will be deployed worldwide, it is important that any customers of the system are assured that Arcta Solutions Limited have a strong and ongoing commitment to cyber security. To help us achieve this, please advise on any relevant internationally recognised certifications and how to obtain them.* *Expected input and dependencies on Arcta Solutions to facilitate the testing.*	**40%**
Experience	*Does the supplier have the relevant skills, experience, and contextual understanding to deliver this work?* *Company background and experience in cybersecurity testing.* *References from previous clients especially where those clients have a similar system or are in the medical field would be beneficial.*	**20%**

Delivery Plan and Risks	*Communication*: Is there a good plan for communicating with the Wellcome team? *Delivery plan*: Is the proposed delivery plan appropriate and achievable? *Feasibility*: How feasible is the delivery plan? Are there significant risks associated with the proposed timelines, and how well are they mitigated?	**25%**
Budget	*Value for Money*: Is the proposed work within your budget and good value for money? Are you able to break down costs per component of work delivered?	**10%**
EDI	*Do they have EDI policies and are these being put into practice in the proposal?*	**5%**
	TOTAL	**100%**

Supplier Interviews

Following a submission of the proposal successful proposals will be invited to a virtual meeting which will last 50 minutes in total and will be a PowerPoint presentation followed by questions and answers session.

6. About Wellcome

Wellcome improves health for everyone by funding research, leading policy and advocacy campaigns, and building global partnerships. Collaborative research that involves a diverse range of people from different fields of interest is key to progress in health science – and to achieving our aim of fostering a healthier, happier, world. We're taking on the biggest health challenges facing humanity – climate and health, infectious disease, and mental health – to find urgent solutions and accelerate preventions. Find out more about Wellcome and our work at: wellcome.org.

7. Prospective Suppliers Personnel - IR35 and Off Payroll Working Rules

Before the RFP response deadline, Prospective Suppliers must make the Wellcome Contact aware if they are intending to submit a proposal where the services will be provided by any individuals who are engaged by the Prospective Supplier via an intermediary i.e.

- Where the Prospective Supplier is an individual contracting through their own personal services company; or
- The Prospective Supplier is providing individuals engaged through intermediaries, for the purposes of the IR35 off-payroll working rules.

8. Equity Diversity and Inclusion

Embracing diversity and inclusion is fundamental to delivering our mission to improve health, and we are committed to cultivating a fair and healthy environment for the people who work here and those we work with. We want to cultivate an inclusive and diverse culture, and as we learn more about barriers that disadvantage certain groups from progressing in our workplace, we will remove them.

Wellcome takes diversity and inclusion seriously, and we want to partner with suppliers who share our commitment. We may ask you questions related to D&I as part of our RFP processes.

9. Accessibility

Wellcome is committed to ensuring that our RFP exercises are accessible to everyone. If you have a disability or a chronic health condition, we can offer adjustments to the response format e.g., submitting your response in an alternate format. For support during the RFP exercise, contact the Wellcome Contact.

If, within the proposed outputs of this RFP exercise, specific adjustments are required by you or your team which incur additional cost then outline them clearly within your commercial response. Wellcome is committed to evaluating all proposals fairly and will ensure any proposed adjustment costs sit outside the commercial evaluation.

All our content should be WCAG 2.2. AAA compliant. Any documents being provided to Wellcome must pass accessibility requirements. If you are unable to produce accessible documents, budget must be set aside to employ a suitable agency to do this work.

10. Independent Proposal

By submission of a proposal, prospective Suppliers warrant that the prices in the proposal have been arrived at independently, without consultation, communication, agreement or understanding for the purpose of restricting competition, as to any matter relating to such prices, with any other potential supplier or with any competitor.

11. Funding

For the avoidance of doubt, the output of this RFP exercise will be funded as a **Contract** and not as a Grant.

12. Costs Incurred by Prospective Suppliers

It should be noted that this document relates to a Request for Proposal only and not a firm commitment from Wellcome to enter into a contractual agreement. In addition, Wellcome will not be held responsible for any costs associated with the production of a response to this Request for Proposal.

13. Sustainability

Wellcome is committed to procuring sustainable, ethical and responsibly sourced materials, goods and services. This means Wellcome seeks to purchase goods and services that minimise negative and enhance positive impacts on the environment and society locally, regionally and globally. To ensure Wellcome's business is conducted ethically and sustainably, we expect our suppliers, and their supply chains, to adhere to these principles in a responsible manner.

14. Wellcome Contact Details

The single point of contact within this RFP exercise for all communications is as indicated below;

Name:	Hardip Dhaliwal
Pronouns:	She/Her
Role:	Procurement Officer
Email:	RFP@wellcome.org