Terms of Reference

Cyber Security Expert

COVID19 Payments: South Africa Rapid Response Incubator Project

10 May 2021

Prepared by FinMark Trust

FinMark Trust

Sanofi House, Second Floor, 44 on Grand
Central Office Park, 2 Bond Street, Grand
Central Extension 1 (Midrand), P.O. Box 61674,
Marshalltown, 2107, South Africa

www.finmark.org.za
T +27 (0) 11 315 9197
info@finmark.org.za

1. About FinMark Trust

FinMark Trust (FMT) is an independent trust whose purpose is to make financial markets work for the poor by promoting financial inclusion and regional financial integration. FMT does this by conducting research to identify the systemic constraints that prevents consumers from accessing financial markets, and by advocating for change based on research findings. Thus, FMT has a catalytic role, driven by its purpose to start processes of change that ultimately lead to the development of inclusive financial systems that can benefit all sectors.

2. Background and contextual information

FMT in partnership with the South African Social Security Agency (SASSA) and the Bill and Melinda Gates Foundation (BMGF) have developed a project aimed at improving access to and usage of grants, particularly for vulnerable groups and women in South Africa. Drawing learnings from the implementation of the temporary Covid-19 SRD grant distribution process the project will seek to design a modified and improved grant distribution system which will enable SASSA to better serve its customers. To achieve this objective the project aims to increase knowledge of grant distribution processes and systems within SASSA by addressing the skills gaps which the organisation currently has and ensuring that skills capacity is retained and developed within the Agency beyond the project.

3. Problem statement

On the 21st April 2020 as part of "Phase 2" of the economic and social relief package the president of South Africa - President Ramaphosa – announced relief measures which South Africans could benefit from to reduce the negative impact caused by the Covid-19 pandemic on their livelihoods. These measures included amongst other (i) the Social Relief of Distress (SRD) Grant for individuals who are unemployed and do not receive any other form of grant or Unemployment Insurance Fund (UIF) payment; (ii) tax relief for businesses; (iii) loans and debt-restructuring for SMMEs, and (iv) an increase in the value of the existing social grants.

The introduction of the SRD grant meant that the South African social grant system would temporarily be expanded. SASSA as the agency responsible for the management and administration of the social grant system in South Africa was tasked with the implementation of this new SRD grant. To ensure the effective and efficient implementation of the SRD grant it was required that SASSA redefine its current business processes and adopt new processes which would enable the organisation to deliver on this expanded mandate. The adoption of these new processes brought to the fore skills gaps/shortages within the organisation. This includes cyber security functions which are currently inadequately addressed by the current staff composition.

4. Objectives

SASSA manages large volumes of sensitive personal and transactional data and requires the integrity, confidentiality and accessibility of the data and the supporting systems. To achieve this, it is imperative that a strong security function be established to safeguard the data environment and the distributed use and acquisition of the data. The consultant will thus be

tasked with establishing an overall security policy and identifying specific security solutions, including ensuring adequate and evolving measures to deal with cyber security. In delivering the above the consultant should further ensure that the Agency has the necessary skills and knowledge required to the implement the policy and identified solution.

5. Scope of Work

FinMark Trust seeks the services of a consultant with in-depth knowledge of data security requirements, policy and strategy/plans development for the Covid19 Payments: South Africa Rapid Response Incubator project. This will entail:

5.1. An assessment of SASSA's current ICT security environment with considerable focus on data/information security.
5.2. An assessment of the global best practice data security/ cyber security strategies/plans and extracting lessons where applicable to improve SASSA's cyber/data security environment.
5.3. A review of previous research conducted on the SASSA cyber/data security environment and extracting any findings/ recommendations which will be useful for this project.
5.4. Based on the assessment and review detailed above design a new cyber/data security policy and strategy/plan and identify specific security solutions.
5.5. Conduct a gap analysis which will direct the Agency to move from its current state to the desired "new process" state and develop a plan to address gaps identified including skills and knowledge gaps. This analysis should also highlight interdependencies with other project workstreams and assign ownership within SASSA.

6. Deliverables

6.1. A comprehensive report detailing the assessments and recommendation for a new/modified data/cyber security strategy/plan.
6.2. A gap analysis report and a detailed plan to address the gaps with indicative timelines.
6.3. A presentation on the above which will be presented to the project team.

7. Proposal Content

Organisations/individuals should submit a detailed technical and financial proposal. The proposal is expected to be clear and concise and should be **no more than 10 pages** and should include:

- A summary of the approach to be implemented in conducting the assessment;
- A detailed timeline for executing all project activities;
- A comprehensive list of anticipated project risks and contingency plans;
- Evidence of technical capacity to undertake this study;
- Name and qualifications of staff members responsible (i) for overseeing the work; (ii) for undertaking the work;
- Detailed costing for each activity, broken down by professional fees and expenses.

8. Safeguarding

The selected service provider has the responsibility to consider and be aware of potential safeguarding issues and the project's potential to integrate gender dimensions and contribute to the advancement of gender equality in addressing the Terms of Reference and be able to demonstrate due diligence in relation to the protection and safeguarding of children and vulnerable groups as per strategies designed to support and manage ongoing risk and abuse, exploitation or neglect of participants in this research project.

9. COVID-19

The selected service provider and FinMark trust recognize the need to minimize the spread of the Corona Virus and the parties will agree on appropriate non face to face methods of communications and completion of required tasks to ensure that work on the project is able to continue effectively. The situation however will be closely monitored by both parties on an ongoing basis.

10. Required skills and qualifications

Applications must provide evidence of the technical capacity to undertake this exercise. This includes capacity to deliver the results in the timeframe provided. Individuals /core team members' CVs must be included, as well as a description of any further resources that may be required. Required skills / qualifications include the following:

- A University ICT related degree (Masters will be advantageous);
- 10 years' work experience in cyber security, ICT security or information security;
- A combination or one of the following industry qualifications CISSP, CISM, CEH, OSCP and GPEN;
- Proven record in developing and implementing security strategies previously;
- Strong skills including knowledge of ICT governance, risk and compliance management;
- Ability to identify vulnerabilities and overall cyber/ information security issues;
- Strong attention to detail with an analytical mind and outstanding problem-solving skills;
- Great awareness of cybersecurity trends and hacking techniques;
- Excellent proven problem solving, communication, interpersonal and facilitation skills.

11. Selection criteria

Contract selection criteria and award will be made based on the following scoring mechanism:

	Criteria	**Weighting**
1	Competence and previous experience	30%
2	Knowledge of cyber and data security	30%
3	Local capacity	10%
4	Budget	30%
	Maximum score	**100%**

12. Submission and timing

Proposals: Proposals for the project should be submitted by close of business on 21 May 2021 at 17:00 (SAST) by email to **Lesego Mashigo, lesego@finmark.org.za**. The successful bidder will be notified by 4 June 2021.

Reporting: The consultant will have two reporting lines. FinMark Trust as the project implementing partner will provide an oversight function and the consultant will report to the FMT team for the duration of the project. As the project relates to functions within SASSA the consultant will also be expected to report to SASSA when conducting the assessment required for the project.

Timing: It is envisaged that the project duration will be **6 months** from the date of contract signature.

The selected consultant must be prepared to meet with FMT on a date to be announced, for a briefing. Once the selection process has been completed, FMT will issue a contract confirming the appointment of the consultant. Any queries relating to the preparation of the application should be referred to **Lesego Mashigo, lesego@finmark.org.za**.

In line with FMT's policy of transparency, answers to queries from one candidate will be circulated to all who indicated their intention to submit a proposal.

Guidance notes to bidders

FinMark Trust reserves the absolute right to use its discretion in the interpretation of these award criteria. The following notes are intended to provide broad guidance only on how proposals will be evaluated. Bidders may be required to clarify their proposals by way of a telephone call or presentation.

"Relevant, demonstrated competence of firm(s) in this area" - you should aim to demonstrate how the firm's collective past experience can be applied (or adapted) to address the specific brief set out in the terms of reference. You are welcome to describe the firm's general experience of financial sector development issues (e.g. in other geographies or topical areas) but the evaluation will focus particularly on the application of that experience for the specific task at hand.

"Demonstrated expertise of key individuals to be involved in this project" – the evaluation places considerable emphasis on the role and demonstrated expertise (i.e. track record) of the key individuals to be involved on the project rather than on the expertise of the firm itself.

"Use of local professional capacity (consulting, analysis, coordination etc.)" – FinMark Trust wishes to ensure that local capacity is used and developed. International firms are therefore encouraged to partner with local organisations.

"Content, quality and originality of proposal" – proposals should address the brief set out in the terms of reference in a comprehensive manner. Bidders should aim for innovation as well as professional presentation. Whilst similar, relevant experience in other markets will be an advantage for a bidder, each market is different and so proposals need to reflect the particular characteristics of that market, as well as the challenge set by the terms of reference.

"Fee basis" – value for money, as well as absolute cost, will be taken into account.

13. **Important to note**

If no communication has been received from FMT after 1 month of your submission, please consider yourself as unsuccessful.