MINUTES OF THE
BRIEFING SESSION FOR RAF/2013/00043 – ICT SECURITY SERVICES

Date	**6 DECEMBER 2013**	**Time**	**10H00**
Venue	**Menlyn Boardroom**	**Facilitator**	**Lee Zietsman (LZ)**

PRESENT	APOLOGIES
See Attendance Register	None

No	SUBJECT MATTER, DETAILS & RESOLUTION

1. Opening and Welcome

LZ welcomed all bidders and made introductions of RAF staff

2. Agenda

- Welcome and Introduction
- Background to Bid
- Purpose of Bid
- Evaluation Criteria
- Functional/Technical criteria
- Mandatory Questions and Documents
- Pricing
- Reasons for disqualification
- Submission of bids
- Contacts
- Questions and Answers

3. Presentation

Dinesh Govender (DG) from the RAF ICT Department explained the background details to the bid request. DG explained the Cisco and firewall concerns and elaborated on the best practices that will need to be enforced in the security of all ICT security alerts. The bidder will be required to manage, patch and monitor security issues,

and advise the RAF via recommendation and reporting. The security service is a 24/7 and 365 days a year support request. Pentesting will be required at regular intervals. The aim is to identify vulnerabilities, however patching must be minimal.

Regarding the Awareness campaign, requires ongoing communication to staff but must also be measurable.

The Project manager must understand all three areas of the ICT Security Request. There could be a team lead for each request, but when the project manager meets with the RAF management team monthly, the project manager must provide the feedback and must have a clear understanding of what has and is to be conducted.

It will be required that the service provider understands the RAF environment and must use an acceptable, reliable and accredited tool and resource to conduct the ICT security request.

4. Questions and Answers

There were questions raised during the presentation and recorded as follows:

Q1. How does the RAF envision "Incident Management"?
A1. The RAF policies and procedures must be followed, however if such is not in place the service provider can develop such procedures.

Q2. Does the RAF require an Incident Response Team?
A2. Based on the scope of work, the request is a response solution, if an incident team will be part of the solution, once problem has been identified.

Q3. Will the project require a change management process and / or a security awareness campaign?
A3. This is a two year contract. The requirements are to assess, test and make recommendations; this is rather an improvement on current situation. On the Security Awareness, the requirements are as per the specification and the service provider must in the two year period manage the awareness campaign and ensure that all RAF Staff are exposed to Security Awareness.

Q4. With regards to pentesting, how is this to be done?
A4. It is required that technical assessments / scans be conducted. Tools are to provide reporting.

Q5. The part of Development for new development, will this be in-house and same codes?
A5. The RAF has an in-house development team. The RAF has not made the distinction, but the network security architecture is in place as well as controls, but they are not restricted.

Q6. Pricing: Could a pricing be supplied on a scale, e.g. price for persons 1 – 50 etc.
A6. Yes, this can be added in the comments, or an additional price scale price list can be attached to the bid. This way the RAF may benefit from the prices, more persons training fro awareness, the cheaper the rate.

It was further mentioned that all questions can be emailed to leeziets@raf.co.za by the latest Friday 13th December 2013.

5. Closure

LZ thanked the bidders for their attendance. The meeting was adjourned at 11h30am.