

SINGAPORE POLICE FORCE

# PLRD dialogue with SAS & ACSA on SAGE 2019 criteria

8 May 2019 PLRD Conference Room

#### <u>Issue 1</u>

What are the types of wireless voice communications system recognized by PLRD for criterion 3.2.2?

#### PLRD's Response

- PLRD cannot prescribe what make/model the security industry can use for obvious reasons
- Besides iDen, there are other 2-way radio communication solutions available in Singapore
- The only objective criterion which PLRD can impose is that the 2-way radio communication system must require a licence from IMDA
- As per PLRD's email dated 24 Apr 2019:
  - if the SA procures the system and is the IMDA licence holder, it must produce the IMDA licence to the assessors for verification during the Main Office assessment
  - if the SA had subscribed to the use of such a system, it must produce the agreement with the 3rd party vendor for verification by the assessors

## **Issue 2** For Criterion 3.2.2, can a communication system which serves only 1 site meet the requirement?

Areas of Audit	Remarks/Observations (To tick or circle where appropriate)		
3.2.2 Does the SA have a wireless voice	Score System (max 10 pts)	pt	
communications system to support its ground operations?	Evidence of a wireless voice communications system in place. (Eg: Non-mobile phones)	10	
Evidence of a wireless voice communications system to support its ground operations.	Evidence of mobile phone as wireless voice communications	8	
(Examples would include mobile phones, dedicated walkie-talkies and IDEN system.)	No evidence of wireless voice communication provided	0	
Assessors may ask for a demonstration of the system.	Assessor's Observation		
Points will be awarded as long as the system is capable of transmitting and receiving voice communications from the ops room to the ground and vice-versa in real time.			
Security officer and ops room operator must demonstrate communication check successfully in the presence of the assessor.			

#### PLRD's Response

 As long as the 2-way radio communication system requires a licence from IMDA, it would meet the criterion

#### Issue 3

For criterion 1.1.19, should a security agency submit evidence for only 1 site or all sites if it has multiple sites?

Areas of Audit	Remarks/Observations (To tick or circle where appropriate)		Points Awarded
1.1.19 Are supervisory checks carried out on	Score System (max 10 pts)		
Security Officers during the assessment period (1 <sup>st</sup> June 2018 to 31 <sup>st</sup> May 2019)? Documents submitted must contain the	Evidence showing one supervisory check was carried out once a month for 12 months from 1 Jun 2018 to 31 May 2019, and the dates tallied with the roster	10	
Illowing: Supervisory Check Roster for all 12 months of the assessment period. Evidence showing that supervisory checks were conducted based on the Supervisory Check Roster must be submitted. Examples of evidence are Occurrence Book, Supervisory Check Book, or any other documentary records.	Evidence showing one supervisory check was carried out once a month for at least 9 months from 1 Jun 2018 to 31 May 2019, and the dates tallied with the roster	8	
	Evidence showing one supervisory check was carried out once a month for at least 5 months from 1 Jun 2018 to 31 May 2019, and the dates tallied with the roster	4	
	All other situations that do not meet the requirements above	0	

- The criterion for 1.1.19 has been amended
- Security agencies will only need to submit the supervisory check rosters for all 12 months of the assessment period for all deployment sites.
- During the main office assessment, the assessors will conduct the assessment based on the evidence of the supervisory checks conducted presented by the security agencies.
  RESTRICTED

#### Issue 4

What are some examples of the technology solutions for criterion 3.1.1?

	(B) TECHNOLOGY SOLUTION Describe how the technology has supported the redesign of this job (15 points)
(i)	What was the proposed technology to be implemented?
	Mobile-enabled Patrol & Incident Management System
	Automated Visitor Management System
	Onsite Surveillance and Analytics
	Clustered Security Guarding
	Risk/Threat Prediction & Detection
	Wearable Security Technology
	Surveillance Robots/ Unmanned Aerial Vehicle
	Virtual Reality (VR)/ Augmented Reality (AR) for Training

Security Collaboration Platform

Others:

The technologies listed above are not exhaustive. SAs are free to cite any technology they have implemented.

- The 9 categories of technologies listed in Section B(i) are illustrative (i.e. not exhaustive)
- There is checkbox for "Others" SAs can cite any solution which does not fall under any of the 9 categories
- SAs are free to cite any technology they had used to support the job re-design
- SAs do not need to limit themselves to the solutions spelled out in the "Security Digital Map"
- The approach is consistent with criterion 3.1.1 in SAGE 2018; PLRD did not stipulate any specific technology solution SAs must employ

#### <u>Issue 5</u>

For criterion 3.1.1, are points awarded based on the number of technologies and/or type of technologies adopted by security agency?

(ii)	Has the	technology	solution	been	implemented?
------	---------	------------	----------	------	--------------

Yes (Date of Implementation: \_\_\_\_\_)

No [If No, to answer (iii) below]

(iii) Why was the technology not implemented?

Clients refused to implement technology

Insufficient funding or in the process of obtaining funding

Other	reasons:	

SAs must provide evidence to support the reason given why the technology was not implemented.

(iv) Describe how the technology has supported the redesign of this job. (Maximum 500 words)

- SAs need only cite one technology which had been used to support the re-design of the SO's job
- As explained earlier, SAs are free to cite any technology they had used to support the job re-design

#### <u>Issue 6</u>

Criterion 3.1.1 appears to be a submission based on quality of write-up which is unfair to a security agency who does not have a staff who can write well

- During the industry consultation sessions in Jan and Feb 2019, we had briefed the industry representatives about this in one of the key thrust
- We are not looking for writing skills; rather, we are looking at how SAs have re-designed an SO's job by weaving in technology to enhance productivity
- To facilitate submission, we have provided a clear template to guide SAs on how to go about putting up the submission

### **SAGE 2019: Policy Direction – Key Thrusts**

#### **1. Increase Emphasis** on Systems Category

- Weightage for the Systems category will be increased
- Weightages for the rest will be correspondingly reduced
- Renamed 'Systems & Technology' to reflect growing emphasis on technology

2. Shift From Output to Outcome-Based Assessment

- Reduce reliance on output-based criteria
- More stringent requirement and assessment
- Increase outcomebased criteria with greater weightage

3. Job Re-Design to Weave in Technology for Productivity

- Job Re-Design to cater to general profile of SOs
- Weaving in of technology in the security processes to enhance productivity

#### <u>Issue 7</u>

It appears that SAs would be able to meet criteria 3.2.2 and 3.1.1 by acquiring the technologies. In this regard, the grading has become more about how rich an SA is rather than how competent. Therefore, PLRD should award "bonus points" for these criteria so that SAs would not be unfairly prejudiced.

- As the industry is aware, the final grades for SAGE 2019 will be decided via a curve
- Hence, the suggestion to award "bonus points" does not address the concern
- More fundamentally, as PLRD has explained many times, our intention is to evolve the grading criteria to sharpen the distinction between SAs which had invested in technology to cut reliance on manpower and SAs which had not

#### Issue 8

The finalized assessment criteria were disseminated in April 2019 while the assessment period runs from 1 June 2018 to 31 May 2019. As such, the grading criteria appears to be applied retrospectively which may be a procedural impropriety. This is regardless that the criteria have not changed much from the previous years, as regulated companies should only be expected to look at confirmed criteria and not expired criteria.

- The annual grading exercise is not a compliance audit
- In other words, PLRD is not measuring how much an SA is complying with a set of published standard
- PLRD's objective is to leverage on the grading exercise to nudge the industry as a whole to move in a certain direction
- PLRD recognizes the SAs' anxiety and will endeavour to start the industry consultation earlier



#### SINGAPORE POLICE FORCE

## **For Discussion**