Notes:

- *This report has been translated into Chinese. If there is any inconsistency between the English version and the Chinese version, the English version shall prevail.*
- *Considered the importance of information security, those not appropriate to be disclosed including the internal details of the system, are redacted.*

SRAA Verification Report

for

Multi-functional Smart Lampposts and Associated Devices of the Office of the Government Chief Information Officer

Version 1.0
12 November 2020

Document Information

Project Name:	Security Risk Assessment and Audit for Multi-functional Smart Lampposts and Associated Devices of the Office of the Government Chief Information Officer		
Document Version Date:	12 November 2020	**Document Version No:**	1.0
Quality Review Method:	Independent Quality Review		

Distribution List

To	Action*	Date	Phone/Fax
OGCIO	Review	12 November 2020	

** Action Types: Approve, Review, Inform, File, Action Required, Attend Meeting, Other (please specify)*

Version History

Ver. No.	Ver. Date	Description	Filename
1.0	12 November 2020	Final Version	OGCIO SRAA Verification Report v1.0.docx

Table of Contents

Abbreviation

The following abbreviations are commonly used in this document:

HKSARG	The Government of the Hong Kong Special Administrative Region
IT	Information Technology
OGCIO	Office of the Government Chief Information Officer
System	Multi-functional Smart Lampposts and Associated Devices
SA	Security Audit
SRA	Security Risk Assessment
SRAA	Security Risk Assessment and Audit
SSL	Secure Socket Layer
The Project team	The independent third party assessor/auditor

1. Project Background

The following services was provided for the Office of the Government Chief Information Officer (OGCIO) of the Government of the Hong Kong Special Administrative Region (HKSARG or the Government):

(a) To evaluate the security risks of the Multi-functional Smart Lampposts and Associated Devices (the System), identify and recommend safeguards with the aim of strengthening the security protection of the system and the related data to an acceptable level.

(b) A verification process will be carried out to review the security status of the system(s) and data to ensure that all risks identified in the security risk assessment and security audit have been mitigated or reduced to an acceptable level.

The scope of the services shall cover the security areas and controls specified in Baseline IT Security Policy (S17), in particular the 14 areas listed in section 2.1 of S17.

The purpose of this document is to formally present the implementation status of recommendations of the security risk assessment and audit activities of the System.

1.1 Security Audit Status Definitions

In the Security Risk Assessment (SRA) stage, each risk finding came with a corresponding recommendation. In the Security Audit (SA) stage, The Project team checked the implementation status of recommendations and discussed the current progress with OGCIO. The individual rectification status could be either:

- **Completed**: the status review found that the recommended safeguard was properly implemented or compensating controls were taken such that the risk was properly rectified;
- **In-Progress**: OGCIO was still implementing recommendations to rectify the risk. Possible reasons were procurement, extended construction work or testing work, as well as involvement of other government departments.
- **Acknowledged:** OGCIO had considered all options of recommended safeguard and concluded that accepting the security risk was the best choice. Typical reasons for this status were relating to rectification cost/resource justification, or integration to environment(s) that could not be controlled by OGCIO, or risk accepted.

1.2 Security Audit Objectives and Scope

The security audit objectives for this work assignment is to perform verification check on the security status after implementation of safeguards to ensure that all vulnerabilities discovered in the last security risk assessment have been fixed and solved with regard to the recommendations provided in the Security Risk Assessment Report, and recommend alternative safeguards for improvement, if applicable.

2. Verification Methodology

2.1 Planning

The Detailed Project Plan was prepared to outline the planning of security audit exercise.

2.2 Information Gathering

The major tasks performed in the information gathering included document review, site visits, vulnerability scan, system configuration reviews and discussions.

2.3 Control Review

The Project team discussed the follow-up actions with OGCIO on the suggested security controls according to the recommendations in the security risk assessment.

2.4 Tests

The Project team reviewed the modified technical security controls according to the recommendations in the security risk assessment.

2.5 Reporting

Each assessment finding in the Security Risk Assessment and Audit Report came with a corresponding recommendation. In the security audit stage, the Project team reviewed the rectification status of the recommendations and discussed the current progress with OGCIO. The individual rectification status could be either:

- **Completed**: the status review found that the recommended safeguard was properly implemented or compensating controls were taken such that the risk was properly rectified.
- **In-Progress**: OGCIO was still implementing recommendations to rectify the risk. Possible reasons were procurement, extended construction work or testing work, as well as involvement of other government departments.
- **Acknowledged:** OGCIO had considered all options of recommended safeguard and concluded that accepting the security risk was the best choice. Typical reasons for this status were relating to rectification cost/resource justification, or integration to environment(s) that could not be controlled by OGCIO, or risk accepted.

The Project team then prepared this security audit report to document the findings and analysis results during the security audit.

2.6 Clean Up and Follow Up

After the security audit report is accepted, sensitive information will be returned to OGCIO or destroyed.

3. Verification Summary

In the security risk assessment and audit, there were 4 medium risk, 11 low risk and 5 AOI item findings on the System described in the Security Risk Assessment and Audit Report.

Table 1. Rectification Status of Host and Network Scan

	Total	High Risk	Medium Risk	Low Risk	AOI
Number of completed rectification	**4**	0	4	0	0
Number of rectification in-progress	**10**	0	0	8	2
Number of acknowledged rectification	**0**	0	0	0	0
Total number of rectification	**14**	**0**	**4**	**8**	**2**

Table 2. Rectification Status of General Control Review

	Total	High Risk	Medium Risk	Low Risk	AOI
Number of completed rectification	**2**	0	0	1	1
Number of rectification in-progress	**4**	0	0	2	2
Number of acknowledged rectification	**0**	0	0	0	0
Total number of rectification	**6**	**0**	**0**	**3**	**3**

3.1 Host and Network Scan Findings:

Report Title	Report Risk	S17 Domain	Description	Verification Status
[redacted]	Low	Access Control	[redacted]	In-Progress Target to complete by Jan of 2021.
	Low	Systems Acquisition, Development and Maintenance		In-Progress Target to complete by Jan of 2021.

[redacted]	Low	Cryptography	[redacted]	In-Progress Target to complete by Jan of 2021.
	Low	Cryptography		In-Progress Target to complete by Jan of 2021.
	AOI	Communications Security		In-Progress Target to complete by Jan of 2021.

[redacted]	Medium	Systems Acquisition, Development and Maintenance	[redacted]	Completed
	Medium	Communications Security		Completed
	Medium	Access Control		Completed
	Medium	Systems Acquisition, Development and Maintenance		Completed

[redacted]	Low	Operations Security	[redacted]	In-Progress Target to complete by Jan of 2021.
	Low	Operations Security		In-Progress Target to complete by Jan of 2021.
	Low	Operations Security		In-Progress Target to complete by Jan of 2021.

[redacted]	Low	Systems Acquisition, Development and Maintenance	[redacted]	In-Progress Target to complete by Jan of 2021.
	AOI	Communications Security		In-Progress Target to complete by Jan of 2021.

3.2 General Control Findings

Report Title	Report Risk	S17 Domain	Description	Verification Status
[redacted]	Low	Physical and Environmental Security	[redacted]	In-Progress Target to complete by Jan of 2021.
	Low	Access Control		Completed
	AOI	Asset Management		Completed
	AOI	Systems Acquisition, Development and Maintenance		In-Progress Target to complete by Jan of 2021.
	Low	Access Control		In-Progress Target to complete by Jan of 2021.

[redacted]	AOI	Cryptography	[redacted]	In-Progress Target to complete by Jan of 2021.

4. Executive Summary

In conclusion, OGCIO had taken necessary actions to evaluate and/or implement all the recommendations for the System in the Security Risk Assessment and Audit Report. No High risks were observed from this security risk assessment and audit. All identified risk findings had been reviewed by OGCIO and safeguards had been planned to be completed by Jan of 2021. It was concluded that the security level for the System is **Satisfactory**.

Appendix I. References

This appendix presents the list of reference materials used in this engagement and the reference materials that OGCIO could refer to in implementing the security safeguards and/or understand this report.

Information Security Standards

- Security Regulations of the HKSARG
- Baseline IT Security Policy [S17]
- The HKSARG Interoperability Framework
- IT Security Guidelines [G3]

General Security Information

- CERT Coordination Center: A major reporting center for Internet security problems.
  http://www.cert.org/
- Common Vulnerabilities and Exposures Project: CVE aims to standardize the names for all publicly known vulnerabilities and security exposures.
  https://cve.mitre.org
- Security Focus: Security Focus is the most comprehensive and trusted source of security information on the Internet. Security Focus is a vendor-neutral site that provides objective, timely and comprehensive security information to all members of the security community, from end users, security hobbyists and network administrators to security consultants, IT Managers, CIOs and CSOs.
  https://www.securityfocus.com/
- Open Source Web Application Security Project: OWASP creates an open source community where people could advance their knowledge about web application and web services security issues by either contributing their knowledge to the education of others or by learning about the topic from documentation and software produced by the project.
  http://www.owasp.org/

~~ End of SRAA Verification Report ~~