Hong Kong Internet Registration Corporation Limited
香港互聯網註冊管理有限公司

Request for Proposals
on
IDS/IPS System

Version 1.0
Date: 11 February 2015

Hong Kong Internet Registration Corporation Limited

Unit 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central,
Sheung Wan, Hong Kong.
Tel.: +852 2319 1313 Fax: +852 2319 2626
Email: enquiry@hkirc.hk Website: www.hkirc.hk

IMPORTANT NOTICE

Table of Contents

1. Summary 1
2. Definitions 2
3. About HKIRC 3
4. The Required System Services 4
4.1. General Requirement 4
4.2. System Requirement 4
4.2.1 Network Intrusion Detection System (NIDS) 4
4.2.2 Network Intrusion Prevention System (NIPS) 6
4.2.3 Phase 1 Baseline Requirements 7
4.2.4 Phase 2 Planned Requirements 8
4.3. Professional Service 9
4.4. Security Incident Mitigation Consultancy Service 9
4.5. Service Location 9
5. Information Security 10
6. Project Acceptance 10
7. Anti-collusion 11
8. Offering Advantages 11
9. Ethical Commitment 12
9.1. Prevention of bribery 12
9.2. Declaration of Interest 12
9.3. Handling of confidential information 13
9.4. Declaration of ethical commitment 14
10. Schedule 15
11. Payment Schedule 16
12. Elements of a Strong Proposal 16
13. Service Agreement Negotiation and Signature 16
14. HKIRC Contacts 17
Appendix A – HKDNR Information Security Policy and Guidelines: An Extract Relevant to Outsourcing 18
Appendix B – Warranty 22
Appendix C – Declaration Form by Contractor on their compliance with the ethical commitment requirements 24
Appendix D – HKIRC Proposal Requirements 26
1.2 Proposal Content 27
1.3 Cover Page 28
1.4 Executive Summary 29

1.5 Conflict of Interest Declaration....29
1.6 Company Background....29
1.7 Methodology....29
1.8 Project Management Methodology....29
1.9 Understanding of our requirements....29
1.10 Knowledge and Advices on Projects/Services....29
1.11 Deliverable and Services level....30
1.12 Proposed Costs of Service and Payment Schedule....30
1.13 Implementation Time Table....30
1.14 Commercial and Payment Terms....30

1. Summary

HKIRC currently providing Doman Name Services for both .hk and .香港 domain. As this service is part of the Critical Internet Infrastructure, security is one of the foremost requirements. In view of a recent surge of Internet attack e.g. Distributed Denial of Service (DDOS), Advanced Persistent Threat (APT) etc. HKIRC is seeking a vendor to implement an Intrusion Detection System and Intrusion Prevention System to mitigate against these threats.

We are planning to implement a system for:

- Continuous network monitoring for all in-bound network traffic
- Continuous network monitoring for all traffic within the De-Militarized Zone (DMZ) and Wide Area Network (WAN)
- Network tread identification and mitigation service customize to HKIRC's environment
- 24x7 emergency support

HKIRC is looking for a solution vendor(s) ("the Contractor") to provide and setup for the above solution.

The system requirement and scope of service is detailed in section 4 of this document.

Parties interested in providing this service shall submit **Expression of Interest (EOI) by 25 February, 2015**. For those who have submitted EOI, they should **submit proposal** (see Appendix D) to the Group **no later than 5:30pm on 18 Mar. 2015**.

The Contractor should submit Expression of Interest by email to HKIRC contacts (refer to Appendix D - HKIRC Proposal Requirements, electronic copy). The Contractor must provide their information as required in the proposal cover page (Appendix D, 1.3 Cover Page).

2. Definitions

The following terms are defined as in this section unless otherwise specified.

“The Contractor” means the company who will provide the Services after award of contract.

“HKIRC” means Hong Kong Internet Registration Corporation Limited.

“HKDNR” means Hong Kong Domain Name Registration Company Limited, a wholly-owned subsidiary of HKIRC, the company requesting the proposal for “the Services”.

“ISMS” means Information Security Management System. It consists of an information security organization and a set of policies, guidelines and procedures concerned with information security management.

“The Services” means the IDS/IPS Implementation Service with requirements stipulated in Section 4 of this document.

“RFP” means this Request for Proposal

“Tenderer” means the company who will submit proposal to provide the Services

3. About HKIRC

Hong Kong Internet Registration Corporation Limited (HKIRC) is a non-profit-distributing and non-statutory corporation responsible for the administration of Internet domain names under '.hk' and '.香港' country-code top level domains. HKIRC provides registration services through its registrars and its wholly-owned subsidiary, Hong Kong Domain Name Registration Company Limited (HKDNR), for domain names ending with '.com.hk', '.org.hk', '.gov.hk', '.edu.hk', '.net.hk', '.idv.hk', '.公司.香港', '.組織.香港', '.政府.香港', '.教育.香港', '.網絡.香港', '.個人.香港'. '.hk' and '.香港'.

HKIRC endeavours to be:

- Cost-conscious but not profit-orientated
- Customer-orientated
- Non-discriminatory
- Efficient and effective
- Proactive and forward-looking

More information about HKIRC can be found at http://www.hkirc.hk .

HKIRC and HKDNR are listed as public bodies under the Prevention of Bribery Ordinance (Cap 201).

4. The Required System Services

4.1. General Requirement

a) Tenderer should provide hardware, software licenses and professional services as a total solution. Partial solution offer will NOT be accepted.
b) Tenderer is required to guarantee the hardware model provided in this tender will not be end-of-support by the original at least five (5) years from the delivery date of that hardware.
c) All proposed equipment must be able to function properly and reliably under the following normal Controlled Environmental conditions:
   i. Temperature 10^{o}C to 50 ^{o}C operating
   ii. Humidity 20%-80% non-condensing
d) All hardware proposed should comply with the Electrical Supply Characteristics list below; otherwise the successful tender is required to provide all necessary construction work in the installation site as specified in section 4.5 of this tender:
   i. The equipment shall be suitable for use on 220 volts +/- 6% 50Hz single phase
   ii. The quality and capacity of all electrical components and cabling shall be fully equivalent to that required by the latest applicable HKSAR Electrical and Mechanical Services Department specifications.
   iii. All equipment shall be fitted with 3-core 13A (Live, Neutral, Earth) fused plug for single-phase industrial type supply cable of 3M in length.
e) All proposed features must be demonstrable during tender evaluation or the proposed equipment will not be accepted otherwise.

4.2. System Requirement

4.2.1 Network Intrusion Detection System (NIDS)

The required NIDS service/solution shall provide:

- A NIDS solution
- Initial installation and configuration for the above
- Consultation and tuning of the NIDS to fitted HKDNR's network environment and requirement

- Sub-sequence solution/system maintenance. 24x7x4, with hardware replacement.
- The NIDS solution should include but not limited to the following features and functions:

    - Detection of vulnerability-based attacks detection including Web (HTTP/HTTPS), Mail, DNS, FTP, WHOIS, SQL server vulnerabilities
    - Detection of Non-vulnerability-based attacks detect based on server resources including:
        - Application DOS – HTTP , SIP, and other flood attacks
        - Authentication defeat - brute force attacks
        - Information theft – application scanning
    - Detection of DOS/DDOS flood attacks that based on network bandwidth resources
    - Detection of Trojan and Phishing attack, targeted as financial fraud, information theft and malware spread.
    - Signatures and behavior based attack detection
    - Support detection alert through EMail, SMS or other out-of-band method or media
    - Provide High-availability to mitigate single point of failure and in case of "inline" network solution, all network should support "failed close", i.e. traffic is to "pass through" device during power off or fail and in case of failure and "failed open", ie. traffic is to block by device during power off or fail.
    - Support multiple network segment detection.
    - Support at least 500Mbps of network traffic and 500,000 concurrent network connections.
    - Support manual and automatic signature update for detection, IP reputation database. Please also state the frequency of these updates.
    - Zero-day attack protection.
    - Support the importing of external rules and signatures, i.e. Snort.
    - Provide availability on add / customize our own rules set.
    - Correlate the results detected by NIDS in both HKDNR data centres.
    - Provide central management function to manage the NIDS in both HKDNR data centres, i.e. administrator can update the NIDS in one single update.
    - Provide performance monitoring capabilities include monitoring of sensor and port throughput utilization and sensor load.
    - Present all threats and system monitoring in form of a dashboard with summary of current threat status.
    - Provide High-availability in the central management function.
    - Correlate the results detected from HKDNR networks equipment.
    - Provide centralize logging function as well as off-device logging to external log servers.
    - Provide report for performance, statistics and management
    - Provide schedule report feature

- Provide different level of report templates, i.e. templates of Standard reports, Executive summary, detailed analysis reports
- Provide availability on customization of the reports

4.2.2 Network Intrusion Prevention System (NIPS)

The required NIPS service/solution shall provide:

- A NIPS System
- Initial installation and configuration
- Consultation and tuning of the NIPS to fitted HKDNR's network environment and requirement
- Sub-sequence solution/system maintenance. 24x7x4, with hardware replacement.
- Analysis and correlation of alert from NIDS to provide advice and mitigation for the intrusion.
- The NIPS solution should include but not limited to the following features and functions:
    - Mitigation through packet/connection throttling, bandwidth control, packet/connection drop
    - Prevention against vulnerability-based attacks detection including Web (HTTP/HTTPS), Mail, DNS, FTP, WHOIS, SQL server vulnerabilities
    - Prevention against non-vulnerability-based attacks detect based on server resources including:
        - Application DOS – HTTP , SIP, and other flood attacks
        - Authentication defeat - brute force attacks
        - Information theft – application scanning
    - Prevention against DOS/DDOS flood attacks that based on network bandwidth resources
    - Prevention against Trojan and Phishing attack, targeted as financial fraud, information theft and malware spread.
    - Support alert through EMail, SMS or other out-of-band method or media
    - Provide High-availability to mitigate single point of failure and in case of "inline" network solution, all network should support "failed close", i.e. traffic is to "pass through" device during power off or fail and in case of failure and "failed open", ie. traffic is to block by device during power off or fail.
    - Support multiple network segment detection.
    - Support at least 500Mbps of network traffic and 500,000 concurrent network connections.

- Support manual and automatic signature update for prevention, IP reputation database. Please also state the frequency of these updates.
- Zero-day attack protection.
- Support the importing of external rules and signatures, i.e. Snort.
- Provide availability on add / customize our own rules set.
- Correlate the results detected by NIPS in both HKDNR data centres.
- Provide central management function to manage the NIDS in both HKDNR data centres, i.e. administrator can update the NIPS in one single update.
- Provide performance monitoring capabilities include monitoring of sensor and port throughput utilization and sensor load.
- Present all threats and system monitoring in form of a dashboard with summary of current mitigation status.
- Provide High-availability in the central management function.
- Correlate the results detected from HKDNR networks equipment.
- Provide centralize logging function as well as off-device logging to external log servers.
- Provide report for performance, statistics and management
- Provide schedule report feature
- Provide different level of report templates, i.e. templates of Standard reports, Executive summary, detailed analysis reports
- Provide availability on customization of the reports

4.2.3 Phase 1 Baseline Requirements

This section document the core functions/features that a vendor's solution shall deliver in the phase 1 implementation. It (a) elaborates the requirements or (b) fills up missing parts in the initial requirement document, and will be used as the baseline requirements of HKDNR during selection process.

1. Intrusion Prevention Capabilities

In phase 1, only intrusion detection (e.g. detect attack and inform us) is focused. Nonetheless, vendor must prove the solution is intrusion prevention ready (e.g. redirect detected DDOS traffic) in current phase. Phase 1 also is divided into sub-phases, sub-phase 1 will implementation for Primary Site only and sub-phase 2 will be implementation for Secondary Site.

2. Secure Cross-Site Data Transfer

Since data would be collected in HKDNR data centres and sent back offsite to vendor's data processing centre. These data are regarded as confidential and should be encrypted before traversing over Internet.

3. Establish Network Baseline

Vendor shall establish network intrusion baseline based on HKDNR requirement and network traffic. This baseline shall be use to form (if)any customization on the IDS/IPS system to prevent any network intrusion to HKDNR's network infrastructure.

4.2.4 Phase 2 Planned Requirements

This section document the core the requirements planned for the next phase implementation. It is a living document and may change with time. It only provides more information to the potential suppliers for resources planning if necessary. This will not form any selection criteria of the phase 1 implementation.

1. Security Monitoring

We are considering to turn on system and audit logging on operating systems, applications, firewall and network equipment wherever available. Security monitoring service should extend to cover the monitoring of these logs to track important security events.

2. Intrusion Prevention Capabilities

In phase 2, intrusion prevention capabilities (e.g. detect DDOS attack, inform us and is capable of blocking the attack) will be enabled, based on the baseline establish in Phase 1. Vendor should only configure the system to block attacks with the consent of HKDNR.

3. System Failover Drill

System Failover Drill should be carryout at both within each site and between each site. The drill shall include but not exclusive to the following functions:

a. Within site failover. The IDS/IPS system with their management element shall still preform their assigned IDS and IPS function should one of the devices failed.
b. Between site failover. Should one of the site fail, the IDS/IPS system with their management element shall still perform their assigned IDS and IPS function.

4.3. Professional Service

Tenderers should be responsible for installation, configuration, and performance tuning. The services provided should be able to fulfil all the specification requirements in Section 4.1 and 4.2.

- One pre-installation meeting should be held before project starts for technical requirement collection. Implementation plan and project schedule should be provided.
- Provide pre-installation checklist, technical advices and assistance in site preparation services.
- Rack-mount installation of appliances, if required. Connect the appliances to network.
- Hardware and software configuration.
- Carry out functional and user acceptance test to assure the products are installed properly according to the requirements.
- Carry out failover drill for within each site and between two sites
- Carry out system tuning based on HKDNR's network infrastructure and equipment.
- Production rollout and monitoring.
- At least one month of nursing period for configuration review, fine-tuning and customize our own rules set.

4.4. Security Incident Mitigation Consultancy Service

The contractor shall provide an optional 24x7 consultancy service for mitigation of security incident for HKDNR. The service shall include:

- Initial security assessment
- Assess extend of intrusion
- Mitigation advice

The contractor are free to propose the charging scheme, ie. either propose a fixed support fee per year or incidents based charges.

The contractor shall provide staff experience background who will be providing the above services.

4.5. Service Location

The Services shall be provided in Hong Kong. The deliverables shall be delivered to the HKIRC's Primary and Secondary facilities.

5. Information Security

The company submitting the proposal ("the company") shall acknowledge and agree that, if the company is selected as the Contractor, it shall be bounded by our Non-Disclosure Agreement (NDA) and Information Security Policy (highlights of the policies are illustrated in Appendix A). The company shall also comply with the obligations under the Personal Data (Privacy) Ordinance and any other obligations in relation to personal data.

The company shall be provided with a set of NDA and Information Security Compliance Statement after HKIRC received the company's Expression-of-Interest before the stipulated time. The NDA and the Information Security Compliance Statement shall be signed and returned to HKIRC attached with documents required by the Compliance Statement before the scheduled deadline. **HKIRC will only consider proposals from companies which have signed both the NDA and the Information Security Compliance Statement.**

The proposal should be marked "RESTRICTED" at the centre-top of each page in black color. It must be encrypted if transmitted electronically.

Each proposal will be reviewed under the terms of non-disclosure by the HKIRC's staff and Board of Directors of HKIRC.

6. Project Acceptance

The overall project acceptance can be broken down into acceptances at various levels:-

1. Delivery, setup and integration of all systems
2. Functionality of individual products
3. Detection and mitigation tune for HKIRC's environment
4. Process and procedures in place and integrated with HKIRC's IT Support Infrastructure
5. System stability observed during the nursing period

7. Anti-collusion

(1) The Tenderer shall not communicate to any person other than HKIRC the amount of any tender, adjust the amount of any tender by arrangement with any other person, make any arrangement with any other person about whether or not he or that other person should or should not tender or otherwise collude with any other person in any manner whatsoever in the tendering process. Any breach of or non-compliance with this sub-clause by the Tenderer shall, without affecting the Tenderer's liability for such breach rules and laws or non-compliance, invalidate his tender.

(2) Sub-clause (1) of this Clause shall have no application to the Tenderer's communications in strict confidence with his own insurers or brokers to obtain an insurance quotation for computation of tender price and communications in strict confidence with his consultants/sub-contractors to solicit their assistance in preparation of tender submission.

(3) The Tenderer shall submit to the HKIRC a duly signed warranty in the form set out in Appendix B to the effect that he understands and will abide by these clauses. The warranty shall be signed by a person authorized to sign the contract on the Tenderer's behalf.

(4) Any breach of any of the representations and/or warranties by the Tenderer may prejudice the Tenderer's future standing as a HKIRC's contractor.

8. Offering Advantages

(1) The Tenderer shall not, and shall procure that his employees, agents and sub-contractors shall not, offer an advantage as defined in the Prevention of Bribery Ordinance, (Cap 201) in connection with the tendering and execution of this contract.

(2) Failure to so procure or any act of offering advantage referred to in (1) above committed by the Tenderer or by an employee, agent or sub-contractor of the Tenderer shall, without affecting the Tenderer's liability for such failure and act, result in his tender being invalidated.

9. Ethical Commitment

9.1. Prevention of bribery

(A) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, except with permission of Hong Kong Internet Registration Corporation Limited (hereafter referred to as the Organisation) solicit or accept any advantage as defined in the Prevention of Bribery Ordinance (Cap 201) in relation to the business of the Organisation. The Contractor shall also caution his directors, employees, agents and sub-contractors against soliciting or accepting any excessive hospitality, entertainment or inducements which would impair their impartiality in relation to the business of the Organisation. The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors are aware of the aforesaid prohibition and will not, except with permission of the Organisation, solicit or accept any advantage, excessive hospitality, etc. in relation to the business of the Organisation.

(B) The Contractor shall not, and shall procure that his directors, employees, agents and sub-contractors who are involved in this Contract shall not, offer any advantage to any Board member or staff in relation to the business of the Organisation.

9.2. Declaration of Interest

(C) The Contractor shall require his directors and employees to declare in writing to the Organisation any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract. In the event that such conflict or potential conflict is disclosed in a declaration, the Contractor shall forthwith take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed. The Contractor shall require his agents and sub-contractors to impose similar restriction on their directors and employees by way of a contractual provision.

(D) The Contractor shall prohibit his directors and employees who are involved in this Contract from engaging in any work or employment other than in the performance of this Contract, with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract. The Contractor shall require his agents and sub-contractors to impose similar

restriction on their directors and employees by way of a contractual provision.

(E) The Contractor shall take all necessary measures (including by way of internal guidelines or contractual provisions where appropriate) to ensure that his directors, employees, agents and sub-contractors who are involved in this Contract are aware of the provisions under the aforesaid sub-clauses (C) and (D).

9.3. Handling of confidential information

(F) The Contractor shall not use or divulge, except for the purpose of this Contract, any information provided by the Organisation in the Contract or in any subsequent correspondence or documentation, or any information obtained when conducting business under this Contract. Any disclosure to any person or agent or sub-contractor for the purpose of the Contract shall be in strict confidence and shall be on a "need to know" basis and extend only so far as may be necessary for the purpose of this Contract. The Contractor shall take all necessary measures (by way of internal guidelines or contractual provisions where appropriate) to ensure that information is not divulged for purposes other than that of this Contract by such person, agent or sub-contractor. The Contractor shall indemnify and keep indemnified the Organisation against all loss, liabilities, damages, costs, legal costs, professional and other expenses of any nature whatsoever the Organisation may suffer, sustain or incur, whether direct or consequential, arising out of or in connection with any breach of the aforesaid non-disclosure provision by the Contractor or his directors, employees, agents or sub-contractors.

9.4. Declaration of ethical commitment

(G) The Contractor shall submit a signed declaration in a form (see Appendix C) prescribed or approved by the Organisation to confirm compliance with the provisions in aforesaid sub-clauses (A) (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and confidentiality. If the Contractor fails to submit the declaration as required, the Organisation shall be entitled to withhold payment until such declaration is submitted and the Contractor shall not be entitled to interest in that period. To demonstrate compliance with the aforesaid sub-clauses (A), (B), (C), (D), (E) and (F) on prevention of bribery, declaration of interest and handling of confidential information, the Contractor and the sub-contractors employed for the performance of duties under this Contract are required to deposit with the Organisation a copy of the internal guidelines issued to their staff.

10. Schedule

	Project schedule Tasks	*To be Completed by*	*Remark*
1	Publish of RFP	16/Feb/2015	
2	Expression of interest	25/Feb/2015	
3	Sign NDA and InfoSec Compliance Statement with all interested vendors	25/Feb/2015	
4	Deadline for vendors to submit proposal and quotation with Warranty Letter	18/Mar/2015, 5:30pm	
5	Director to join Evaluation Team	24/Mar/2015	
6	Selection of vendor by panel	9/Apr/2015	
7	Conclude final decision and appoint the vendor	16/Apr/2015	
8	Prepare contract and service agreement	4/May/2015	
9	Sign contract and service agreement with the appointed vendor	29/May/2015	
10	Delivery of hardware and software	26/Jun/2015	
11	System implementation: Phase 1	24/Jul/2015	
12	System implementation: Phase 2	21/Aug/2015	
13	Nursing Period complete	21/Aug/2015	
14	Project complete with deliverables	21/Aug/2015	

11. Payment Schedule

Interested vendors shall provide the breakdown of the cost, in Hong Kong Dollars, of the whole service specified in the proposal.

The Contractors should make certain that prices quote are accurate before submitting their proposal. Under no circumstances will the HKIRC accept any request for adjustment on the grounds that a mistake has been made in the proposed prices.

The following payment schedule is recommended but interested vendors may propose their own in their proposals.

	Milestone/Acceptance	**Expected duration**	**Payment**
1	(a) Completion of delivery and basic installation of all hardware and software products (b) Acceptance of functionality of individual products	4 weeks	40%
2	(a) Completion of system configuration, functionally ready (b) Completion of Phase 1	4 weeks	20%
3	Completion of Phase 2	4 weeks	20%
4	Acceptance of stability after the nursing period	4 weeks	20%
	TOTAL	**16 weeks**	**100%**

12. Elements of a Strong Proposal

All submitted proposal must following the format as stated in Appendix D - HKIRC Proposal Requirements

13. Service Agreement Negotiation and Signature

The service agreement will be drawn up between the selected vendor and HKDNR, the wholly-owned subsidiary of HKIRC. HKIRC welcomes the vendor's proposal on a suitable service agreement for the project/service.

The service agreement must be signed by both parties within one week from the project/service

award date. If the agreement is not signed within the said period, HKIRC will start the negotiation with the next qualified vendor on the selection list.

14. HKIRC Contacts

HKIRC Contacts information

Contacts	
Hong Kong Internet Registration Corporation Limited Unit 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central, Sheung Wan, Hong Kong +852 23192303 – telephone +852 23192626 – fax http://www.hkirc.hk *If you are not sure about the appropriate person to call, the receptionist can help you.*	**IT Project Manager** Ben Choy +852 23193819 ben.choy@hkirc.hk **IT Manager** Ben Lee +852 23193811 ben.lee@hkirc.hk **CEO** Jonathan Shea +852 23193821 jonathan.shea@hkirc.hk

Appendix A – HKDNR Information Security Policy and Guidelines: An Extract Relevant to Outsourcing

This document provides an extract of the HKDNR Information Security Policy and Guidelines with the purposes of (a) introducing various measures and controls to be executed by HKDNR regarding outsourcing and (b) setting the expectation of any potential contractors that their participation and conformance in these measures and controls are essential contractual obligations.

The original Policy and Guidelines applies to HKDNR's employees, contractors and third party users. However, a potential contractor may interpret the clauses up to their roles and responsibilities only. Nonetheless, the keyword "**contractors**" hereby refers to all relevant staff members of the contractor and those of any other subcontractors under the contractor's purview.

Herein, HKDNR would also set the expectation of any potential contractors that upon their expression-of-interest to the project/service, they shall be required in the subsequent stages (a) to sign off a non-disclosure agreement (NDA) on all information to be provided and (b) to sign off a Compliance Statement where compliance requirements are specified in more details.

(A) Extract from the HKDNR Information Security Policy

In the following, "the organization" means Hong Kong Domain Name Registration Company Limited, the company requesting the proposal for "the Project."

8. Human resources security

8.1 Security objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

8.1.1 Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

8.1.2 Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and

proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 As part of their contractual obligations, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.

8.2 During employment
Security objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

8.2.1 Management shall require employees, contractors and third party users to apply security measures in accordance with established policies and procedures of the organization.

8.2.2 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates on organizational policies and procedures, as relevant to their job functions.

8.3 Termination or change of employment
Security objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

8.3.2 All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

8.3.3 The access rights of all employees, contractors and third party users to information and information processing facilities shall either be removed upon termination of their employment, contract or agreement, or adjusted upon change.

12. Information systems acquisition, development and maintenance
12.5.5 Outsourced software development shall be supervised and monitored by the organization

13. Information security incident management
13.1 Reporting information security events and weaknesses
Security objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action.

13.1.2 All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.

(B) Extract from the HKDNR Information Security Guidelines

6. ORGANIZING INFORMATION SECURITY

6.2 EXTERNAL PARTIES

6.2.1 Identification of Risks Related to External Parties

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting the access.

6.2.3 Addressing Security in Third Party Agreements

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

7. ASSET MANAGMENT

7.1.3 Acceptable Use of Assets

Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

8. HUMAN RESOURCE SECURITY

8.1.1 Roles and Responsibilities

Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.

8.1.2 Screening

Background verification checks on all candidates for employment, contractors, and third party users shall be conducted in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 Terms and Conditions of Employment

As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the

organization’s responsibilities for information security.

8.2.1 Management Responsibilities

Management shall require employees, contractors and third party users to apply security measures in accordance with established policies and procedures of the organization.

12. Information systems acquisition, development and maintenance

12.5.5 Outsourced Software Development

Outsourced software development shall be supervised and monitored by the organization.

Appendix B – Warranty

To: Hong Kong Internet Registration Corporation Limited (HKIRC)

Dear Sir/Madam,

Warranty

(1) By submitting a tender, the Tenderer represents and warrants that in relation to the tender of Network IDS/IPS System:

(i) it has not communicated and will not communicate to any person other than the HKIRC the amount of any tender price;
(ii) it has not fixed and will not fix the amount of any tender price by arrangement with any person;
(iii) it has not made and will not make any arrangement with any person as to whether it or that other person will or will not submit a tender; and
(iv) it has not otherwise colluded and will not otherwise collude with any person in any manner whatsoever in the tendering process.

(2) In the event that the Tenderer is in breach of any of the representations and/or warranties in Clause (1) above, the HKIRC shall be entitled to, without compensation to any person or liability on the part of the HKIRC :

(i) reject the tender;
(ii) if the HKIRC has accepted the tender, withdraw its acceptance of the tender; and
(iii) if the HKIRC has entered into the contract with the Tenderer,
terminate the contract.

(3) The Tenderer shall indemnify and keep indemnified the HKIRC against all losses, damages, costs or expenses arising out of or in relation to any breach of any of the representations and/or warranties in Clause (1) above.

(4) Clause (1) shall have no application to the Tenderer's communications in strict confidence with its own insurers or brokers to obtain an insurance quotation for computation of the tender price, or with its professional advisers, and consultants or sub-contractors to solicit their assistance in preparation of tender submission. For the avoidance of doubt, the making of a bid by a bidder to the HKIRC in public during an auction will not by itself be regarded as a breach of the representation and warranty in Clause (1)(i) above.

(5) The rights of HKIRC under Clauses (2) to (4) above are in addition to and without prejudice to any other rights or remedies available to it against the Tenderer.

Authorized Signature & Company Chop :

Name of Person Authorized to Sign (in Block Letters) :

Name of Tenderer in English (in Block Letters) :

Date :

Appendix C – Declaration Form by Contractor on their compliance with the ethical commitment requirements

To: Hong Kong Internet Registration Corporation Limited (HKIRC)
Contract No.:
Title:

In accordance with the Ethical Commitment clauses in the Contract:

1) We confirm that we have complied with the following provisions and have ensured that our directors, employees, agents and sub-contractors are aware of the following provisions:

   a) prohibiting our directors, employees, agents and sub-contractors who are involved in this Contract from offering, soliciting or accepting any advantage as defined in section 2 of the Prevention of Bribery Ordinance (Cap 201) in relation to the business of HKIRC except with the permission of HKIRC;

   b) requiring our directors, employees, agents and sub-contractors who are involved in this Contract to declare in writing to their respective company management any conflict or potential conflict between their personal/financial interests and their duties in connection with this Contract, and in the event that a conflict or potential conflict is disclosed, take such reasonable measures as are necessary to mitigate as far as possible or remove the conflict or potential conflict so disclosed;

   c) prohibiting our directors and employees who are involved in this Contract from engaging in any work or employment (other than in the performance of this Contract), with or without remuneration, which could create or potentially give rise to a conflict between their personal/financial interests and their duties in connection with this Contract and requiring our agents and sub-contractors to do the same; and

   d) taking all measures as necessary to protect any confidential/privileged information or data entrusted to us by or on behalf of HKIRC from being divulged to a third party other than those allowed in this Contract.

Signature
(Name of the Contractor)
(Name of the Signatory)
(Position of the Signatory)
(Date)

Appendix D – HKIRC Proposal Requirements

Proposal requirements	
Submission deadline	Please refer to Section 10 - Schedule, item no. 4 for the proposal submission deadline. If tropical cyclone warning signal No.8 or above or the black rainstorm warning is hoisted on the deadline date, the deadline will be postponed to the next working day without advance notice.
Delivery address	Hong Kong Internet Registration Corporation Limited Unit 2002-2005, 20/F FWD Financial Centre, 308 Des Voeux Road Central, Sheung Wan, Hong Kong
Hard copies	2 copies of the full proposal are required. The proposal shall be to the attention of Elisa Chung (Finance Officer) or Bonnie Chun (Operation Manager)
Electronic copy	Electronic copy is required, on disk or by email to elisa.chung@hkirc.hk and bonnie.chun@hkirc.hk; also cc ben.choy@hkirc.hk and ben.lee@hkirc.hk. This is not a substitute for the physical copies mentioned above.
Proposal format	Specified in this document
Page count	30 pages or fewer. Stapled. Do not bind.
Font	Electronically published or typed. Times New Roman 12 point font.

Successful vendor is the one who submitted a clearly worded proposal that demonstrates the following attributes:

- a persuasive section on the company background
- international recognize certification for quality assurance
- a strong and flexible service and tools meeting HKIRC requirements with minimum customization
- high level of interaction between HKIRC and the vendor
- excellent fit with the capabilities and facilities of HKIRC
- strong company and project management team

1.2 Proposal Content

The proposal should contain the following:

- Cover Page
- Executive Summary
- Conflict of Interest Declaration
- Company Background
    - Financial Situation
    - Track Records
    - Organization and management team
    - Project team with credentials
    - Company credentials
    - Staff credentials
- Methodology
- Project management methodology
- Understanding of our requirements
- Knowledge and Advices on Projects/Services
- Deliverable and Services level
- Proposed Cost of Services and Payment Schedule
- Implementation Time Table
- Commercial and Payment Terms. e.g. Compensation for delay.

1.3 Cover Page

Prepare a non-confidential cover page with the following information in the order given.

Cover Page		
Project Title		
		IDS/IPS System
Project Manager	Name:	
	Title:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
Company	Contact person:	
	Title:	
	Company name:	
	Mailing address:	
	Phone:	
	Fax:	
	Email:	
	Website:	

1.4 Executive Summary

The executive summary provides a brief synopsis of the commercial and technical solution the vendor proposed for the project/service. This summary must be non-confidential. It should fit on a single page.

The executive summary should be constructed to reflect the merits of the proposal and its feasibility. It should also clearly specify the project/service's goals and resource requirements. It should include:

- Rationale for pursuing the project or service, the methodology/technology needed and the present state of the relevant methodology/technology.
- Brief description of the vendor's financial situation.
- Brief description of the vendor's facilities and experience on similar projects or services

1.5 Conflict of Interest Declaration

Declare any conflict of interest in relation to the project and the '.hk' ccTLD registry HKIRC.

1.6 Company Background

The vendor must describe its company background. Major activities, financial situation, organizational structure, management team and achievements in similar projects/services or service outsourcing of the company should be elaborated. Track records are preferred.

List the key technical and management personnel in the proposal. Provide a summary of the qualifications and role of each key member.

1.7 Methodology

The vendor must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

1.8 Project Management Methodology

The vendor must describe the methods to be used, and briefly explains its advantage and disadvantage. Track records are preferred.

1.9 Understanding of our requirements

The vendor shall describe their understanding of our requirements. With the use of a table, the vendor should clearly state their compliance on the requirements listed in the scope of service section; and briefly explain how they are achieved.

1.10 Knowledge and Advices on Projects/Services

The vendor should describe their knowledge and advices to ensure the success of this

project/service or projects/services with similar nature.

1.11 Deliverable and Services level

The vendor should detail the project/service deliverables, and the services level of the proposed services. Tables of content of all reports included in the deliverables should be provided in the proposal.

1.12 Proposed Costs of Service and Payment Schedule

The vendor should provide the breakdown of the cost of the whole project/service. The cost shall be broken down by milestone/phases. The payment shall be scheduled based on the milestones and/or deliverables.

Such costs should include, if applicable:

- Fixed setup cost
- Labour unit costs for additional services or requirements. They are typically quoted in unit man day. Quoted in normal working hour, non-working hour and in emergency.
- Equipment that is permanently placed or purchased for HKIRC to complete the project or service, if any.
- Subsequent support, maintenance or consultation service.
- Other direct costs including services, materials, supplies, postage, traveling, pocket money, etc.

1.13 Implementation Time Table

The vendor should present in this section the implementation schedule of the project/service. The schedule should be realistic and achievable by the vendor.

1.14 Commercial and Payment Terms

The vendor should describe the commercial and payment terms of the services e.g. compensation for the delay of the project/service.