CREDIT INFORMATION CORPORATION
6F Exchange Corner Building
107 V. A. Rufino Street corner Esteban St.,
Legaspi Village, Makati City 1229
(02) 236-5900 | www.creditinfo.gov.ph

September 17, 2019

REQUEST FOR QUOTATION
ENGAGEMENT OF CONSULTANCY SERVICES FOR
EXTERNAL VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Negotiated Procurement (SVP) No. RFQ19-087

Sir/Madam:

The Credit Information Corporation invites you to submit your quotation / offer for the item/s described below using the **Price Proposal Form (see Annex "A")** subject to the terms and conditions stated in the RFQ and Terms of Reference **(see Annex "B")**

DESCRIPTION	Approved Budget for the Contract
External Vulnerability Assessment and Penetration Testing	₱900,000.00

Submit your proposal, together with the following documents, duly signed by you or your duly authorized representative, not later than **24 September 2019, 5:00 p.m.**

1. **Curriculum Vitae**
2. **Mayor's/Business Permit 2019;**
3. **PhilGEPS Certificate/Number;**
4. **Income Tax Return 2018;**
5. **Notarized Omnibus Sworn Statement (Annex C)**
6. **For Authorized Representatives: SPA (Sole Proprietorship/Partnership), Secretary's Certificate or Board Resolution (Corporation)**

Proposals shall be submitted at the address indicated below:

Administrative Office
Credit Information Corporation
6F, Exchange Corner Bldg., 107 VA Rufino St.
cor. Esteban St., Legaspi Village, Makati City

Only one (1) set of documents certified to be true copies of the original shall be required.

Proposals and other documents required may be sent electronically analiza.chua@creditinfo.gov.ph or orlando.brillantes@creditinfo.gov.ph. Electronically submitted proposals and documents must be submitted on or before the deadline of submission as stated in this RFQ.

Late submission of quotations shall not be accepted and considered.

SGD
TONI ROSE E. UNCIANO
Administrative Services Officer V

N.B.: Suppliers not directly invited may participate. The duly accomplished Proposal (Annex A), together with the other required documents, shall be submitted on or before the deadline for submission of proposal or any extension thereof. The following supporting documents may be submitted anytime during submission of offers, evaluation of offers, before issuance of Notice of Award or prior to payment:

1. Mayor's Permit for the year 2019;
2. PhilGEPS Registration Number; and

PhilGEPS Platinum Registration Certificate may be submitted **in lieu** of the foregoing documents.

ANNEX "A"

PRICE PROPOSAL FORM

Date: _____

Administrative Office
Credit Information Corporation
6F, Exchange Corner Bldg., 107 VA Rufino St.
cor. Esteban St., Legaspi Village, Makati City

Madam:

Having examined the Request for Quotation No. RFQ19-087, which includes the technical specifications/Terms of Reference, the receipt of which is hereby duly acknowledged, the undersigned, offer to, in conformity with the said Request for Quotation for the sums stated hereunder:

ITEM/DESCRIPTION	UNIT PRICE	TOTAL PRICE
External Vulnerability Assessment and Penetration Testing		
	Total Price Proposal	

TOTAL PRICE IN WORDS:

_____

We undertake, if our Proposal is accepted, to deliver the goods/services as identified in the Technical Specifications/Terms of Reference and in accordance with the delivery schedule.

Our quotation includes all taxes, duties and/or levies payable and is valid for a period of THIRTY (30) calendar days upon issuance of this document.

We understand that the CIC Technical Working Group may require from us the submission of documents that will prove our legal, financial and technical capability to undertake this project.

Until a formal Contract is prepared and executed, this Proposal, together with your written acceptance thereof and your Notice of Award, shall be binding upon us.

We understand that you are not bound to accept the lowest or any Proposal you may receive.

Dated this _____.

_____
Signature of Authorized Representative

_____
Printed Name of Authorized Representative

_____
Capacity

Duly authorized to sign Proposal for and on behalf of: _____

Annex C

Omnibus Sworn Statement

REPUBLIC OF THE PHILIPPINES)
CITY/MUNICIPALITY OF _____) S.S.

A F F I D A V I T

I, *[Name of Affiant]*, of legal age, *[Civil Status]*, *[Nationality]*, and residing at *[Address of Affiant]*, after having been duly sworn in accordance with law, do hereby depose and state that:

1. ***Select one, delete the other:***

   If a sole proprietorship: I am the sole proprietor of *[Name of Bidder]* with office address at *[address of Bidder]*;

   If a partnership, corporation, cooperative, or joint venture: I am the duly authorized and designated representative of *[Name of Bidder]* with office address at *[address of Bidder]*;

2. ***Select one, delete the other:***

   If a sole proprietorship: As the owner and sole proprietor of *[Name of Bidder]*, I have full power and authority to do, execute and perform any and all acts necessary to represent it in the bidding for *[Name of the Project]* of the *[Name of the Procuring Entity]*;

   If a partnership, corporation, cooperative, or joint venture: I am granted full power and authority to do, execute and perform any and all acts necessary and/or to represent the *[Name of Bidder]* in the bidding as shown in the attached *[state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate issued by the corporation or the members of the joint venture)]*;

3. *[Name of Bidder]* is not "blacklisted" or barred from bidding by the Government of the Philippines or any of its agencies, offices, corporations, or Local Government Units, foreign government/foreign or international financing institution whose blacklisting rules have been recognized by the Government Procurement Policy Board;

4. Each of the documents submitted in satisfaction of the bidding requirements is an authentic copy of the original, complete, and all statements and information provided therein are true and correct;

5. *[Name of Bidder]* is authorizing the Head of the Procuring Entity or its duly authorized representative(s) to verify all the documents submitted;

6. *Select one, delete the rest:*

   If a sole proprietorship: I am not related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   If a partnership or cooperative: None of the officers and members of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

   If a corporation or joint venture: None of the officers, directors, and controlling stockholders of *[Name of Bidder]* is related to the Head of the Procuring Entity, members of the Bids and Awards Committee (BAC), the Technical Working Group, and the BAC Secretariat, the head of the Project Management Office or the end-user unit, and the project consultants by consanguinity or affinity up to the third civil degree;

7. *[Name of Bidder]* complies with existing labor laws and standards;

8. *[Name of Bidder]* is aware of and has undertaken the following responsibilities as a Bidder:

   a) Carefully examine all of the Bidding Documents;

   b) Acknowledge all conditions, local or otherwise, affecting the implementation of the Contract;

   c) Made an estimate of the facilities available and needed for the contract to be bid, if any; and

   d) Inquire or secure Supplemental/Bid Bulletin(s) issued for the *[Name of the Project]*.

9. *[Name of Bidder]* did not give or pay directly or indirectly, any commission, amount, fee, or any form of consideration, pecuniary or otherwise, to any person or official, personnel or representative of the government in relation to any procurement project or activity; and

10. *[Name of Bidder]* hereby assigns the following contact number/s and e-mail address/es as the official telephone/fax number and contact reference of the company where the CIC BAC and CIC notices may be transmitted.

    Telephone No/s.: _____
    Fax No/s.: _____
    E-mail Add/s.: _____

It is understood that notices/s transmitted in the above-stated telephone/fax numbers and/or e-mail address/es are deemed received as of its transmittal and the reckoning period for the reglementary periods stated in the bidding documents and the revised Implementing Rules and Regulations of Republic Act No. 9184 shall commence from receipt thereof.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of _____, 2017 at _____, Philippines.

_____
Bidder's Representative/Authorized Signatory

SUBSCRIBED AND SWORN to before me this __ day of *[month] [year]* at *[place of execution]*, Philippines. Affiant/s is/are personally known to me and was/were identified by me through competent evidence of identity as defined in the 2004 Rules on Notarial Practice (A.M. No. 02-8-13-SC). Affiant/s exhibited to me his/her *[insert type of government identification card used]*, with his/her photograph and signature appearing thereon, with no. _____ .

Witness my hand and seal this ___ day of *[month] [year]*.

NAME OF NOTARY PUBLIC

Doc. No. ___
Page No. ___
Book No. ___
Series of ____.

Note:

"Sec. 12. Competent Evidence of Identity – The phrase "competent evidence of identity" refers to the identification of an individual based on:

> At least one current identification document issued by an official agency bearing the photograph and signature of the individual, such as but not limited to, passport, driver's license, Professional Regulations Commission ID, National Bureau of Investigation clearance, police clearance, postal ID, voter's ID, Barangay certification, Government Service and Insurance System (GSIS) e-card, Social Security System (SSS) card, Philhealth card, senior citizen card, Overseas Workers Welfare Administration (OWWA) ID, OFW ID, seaman's book, alien certificate of registration/immigrant certificate of registration, government office ID, certification from the National Council for the Welfare of Disabled Persons (NCWDP), Department of Social Welfare and Development (DSWD) certification;

The Board Resolution or Secretary's Certificate referring to the said Board Resolution designating the bidder's authorized representative and signatory need not specifically indicate the particular project where such authority is given provided that the said authority covers activities by CIC.

TERMS OF REFERENCE FOR EXTERNAL VULNERABILITY ASSESSMENT AND PENETRATION TESTING

I. GENERAL INFORMATION

The Credit Information Corporation (CIC) is a Government-Owned and Controlled Corporation (GOCC) created in 2008 by virtue of Republic Act No. 9510 otherwise known as the Credit Information System Act (CISA). The CIC is mandated to establish a comprehensive and centralized credit information system for the collection and dissemination of fair and accurate information relevant to, or arising from credit and credit-related activities of all entities participating in the financial system, such as but not limited to retail, trade, utilities, and other service and product providers that may yield data on creditworthiness and payment behavior.

II. PROJECT BRIEF

The Credit Information Corporation (CIC) anticipates to conduct an information security review of the underpinning systems of its Credit Information System (CIS). Due to the technical nature the project and requirements, the CIC is seeking the assistance of a Professional Security Service firm referred further as the Firm to perform Vulnerability Assessment and Penetration Testing (VAPT) to help CIC achieve the following:

- Gain a better understanding of potential vulnerabilities and threats that may be visible from external network;
- Assess and identify all weaknesses of identified resources;
- Execute non-disruptive attack-simulation to determine weaknesses of target information systems; and

Bidder's/Supplier's Conforme:_____
Signature over Printed Name

- Identify the risk level where CIC is exposed to so that appropriate counter measures can be developed and applied.

The Firm shall undertake all necessary steps, employ suitable strategies, and make available appropriately equipped personnel in all phases of the engagement.

III. SCOPE OF WORK

The scope of this engagement will be limited to external facing network services and underlying internal hosts of the CIC. The security review will be a combination of black-box and grey-box approach.

The Black box approach is a limited knowledge security assessment that simulates a real-life attack against the application from unauthorized users.

The Grey box approach is follow-up assessment to the earlier approach. The Firm will be required to provide their public IP addresses where testing or connection is to originate for white-listing. Detailed information about the target applications will also be provided such as IP addresses, operating system details, server function, and user account to the application;

Below is a list of CIC hosts that will be considered for the security review:

Webserver 1	online.creditinfo.com.ph
Webserver 2	a2a.creditinfo.com.ph
Webserver 3	online-test.creditinfo.com.ph
Webserver 4	www.creditinfo.gov.ph
FTP Server 1	ftp.creditinfo.com.ph

The review will be performed during November to December 2019 ;

IV. REQUIRED ACTIVITIES

The activity will be performed in two (2) passes after the project kick off. Pass 1 will perform the assessment activities below:

Step 1: Reconnaissance: Discover and identify information from the Internet and other available resources, all information that will represent CIC's Internet footprint. Report the information gathered as well as the methodology on how the information was discovered.

Bidder's/Supplier's Conforme:_____
Signature over Printed Name

Step 2: Identify Vulnerabilities: Probe resources (discovered/in-scope) to identify listening services. Identify and assess vulnerabilities that may be present in those exposed services. Produce a prioritized list of security vulnerabilities.

Step 3: Exploit: Attempt to exploit identified vulnerabilities using a combination of automated and manual tests to uncover OWASP Top 10 application security risks:

1) All forms of Injection flaws;

2) Cross-Site Scripting (XSS) which can allow attackers to execute scripts in the victim's browser to hijack user sessions;

3) Security Misconfiguration of the systems involved;

4) Missing Function Level Access Control which can let attackers to forge application requests in order to access functionality in the website without proper authorization;

5) Using Components with Known Vulnerabilities can undermine application defenses and enable a range of possible attacks.

6) Broken Authentication and Session Management can allow attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws.

7) Insecure Direct Object References may allow attackers to manipulate insecurely exposed references to an internal implementation object to access unauthorized data.

8) Sensitive Data Exposure may allow attackers to steal or modify weakly protected sensitive data to conduct fraud, identity theft, or other crimes.

9) Cross-Site Request Forgery (CSRF) allows attackers to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

10) Invalidated Redirects and Forwards allow attackers to redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Step 4: Review of Application Architecture. Attempt to find, download, and review server-side scripts, configuration files, include files and HTML source. Check for issues such as database connection strings, configuration settings, unauthorized directory listings and commented code.

Step 5: Analyze Risk. Evaluate the identified areas of weakness, and rate the findings based on the risk that each pose to the CIC.

Bidder's/Supplier's Conforme:_____

Signature over Printed Name

The Firm will perform a second pass and validate the implementation of the technical review recommendations previously identified in first pass. The activity will be performed after four (4) weeks to allow the CIC implement recommend measures to mitigate identified risks. The Firm shall perform similar procedures as described above.

V. DELIVERABLES

The Firm shall submit and present to CIC's management, based on the scope of work, and in accordance with the timeline, a comprehensive report containing the following:

1) **Submission of a Project Plan.** Project plan detailing all the dates for the work phases, deliverables, review meetings, report delivery and report allocations.

2) **Submission of an Interim Report.** A report in the form of threat and vulnerability matrix that details the description of the vulnerabilities, impact and criticality and recommendation.

3) **Submission of an Executive Report.** An executive summary report detailing the engagement's scope, approach and summary recommendations aimed at senior management. Must contain non-technical descriptions of all findings along with discussions of the inherent business risks and recommended risk management strategies.

4) **Submission of a Technical Report.** A report covering identified security risks, exposures and proposed recommendation aimed at technical staff and should provide them with complete solutions.

5) **Executive presentation.** A presentation of the identified risks to the Cyber Security Committee of the board of directors.

6) **Knowledge Transfer.** A formal training on risk management and risk identification techniques using the OWASP framework.

VI. KNOWLEDGE TRANSFER

OWASP Training. Provide a risk identification training using the OWASP framework from an OWASP certified instructor. The training must not be less than 8 hours. The training must be held at the CIC business office, and will be scheduled on a Friday or Saturday. The training will be attended by eight technical personnel of the CIMS.

Risk Management Training. To enable the trainee gain comprehensive knowledge of the fundamental principles, framework and process of risk management. Meets the requirements of the PECB, covering the following key competency domains:

Fundamental principles and concepts of Risk Management, Risk Management framework and process, Risk assessment techniques based on IEC/ISO 31010

VII. PROJECT TIMELINE

CIC shall engage the services of the Firm for an estimated period of forty five (45) calendar days, subject to extension as warranted. The examination of system shall be undertaken during off-office hours and subject to reasonable guidelines of the CIC. Any amendment/modification of the work schedules shall be made only upon prior written approval of the CIC Technical Working Group, in which case, the engagement shall be correspondingly extended for such period called for by the amendment/modification under the same terms, with no additional cost on the part of CIC. Proposed timeline below:

Activities	W1	W2	W3	W4	W5-7	W8	W9
First pass							
Validation meeting							
Interim report							
Remediation (CIC)							
Second pass							
Validation meeting							
Submission of final reports							
Presentation							
Knowledge transfer							

VIII. APPROVED BUDGET CONTRACT AND TERMS OF PAYMENT

The total contract cost amounts to NINE HUNDRED THOUSAND PESOS (Php900,000.00) which shall be paid in FULL after completion of the Project subject to the acceptance of the deliverables by the Inspection and Acceptance Committee.

IX. QUALIFICATIONS

Professional Security Service Firm

1) Minimum five (5) years of experience in conducting the said activity with financial and government institutions (if possible, provide reference of Government clients).

Bidder's/Supplier's Conforme:_____

Signature over Printed Name

Project Manager

1) Graduate in Computer Engineering, Computer Science, Electrical Engineering, Information Systems, Information Technology, or a closely related Engineering or IT discipline;

2) Certificate in Project Management Professional (PMP) and ITIL would be an advantage.

3) Minimum five (5) years of experience in managing IT Projects, and three (3) years of managing information security audits;

4) Relevant experience in managing projects related to Bangko Sentral ng Pilipinas (BSP) Circular 982 - Enhanced Guidelines on Information Security Management

Security Engineers

1) Graduate in Computer Engineering, Computer Science, Electrical Engineering, Information Systems, Information Technology, or a closely related Engineering or IT discipline;

2) Active certification of at least one of the following GPEN, LPT or OSCP.

3) Three (3) years experience in information security review or audit especially in conducting network layer penetration testing and application layer penetration testing;

4) Ability to perform testing and validation of OWASP Top Ten and other similar application security standards;

Submission of proposals and eligibility requirements shall be made at 6F Exchange Corner Building 107 V. A. Rufino Street corner Esteban St., Legaspi Village, and Makati City 1229.

Prepared by:

MARBIN M. FADRIQUELA
IT Officer III, Technical Support Department

Bidder's/Supplier's Conforme:_____
Signature over Printed Name

Reviewed by:

ARIEL DAJAO
Member

TONI ROSE E. UNCIANO
Member

LADY HANNAH BALANA
Member

DENNYSON HILBERO
Member

ATTY. RYAN ROMEO PEREZ
BAC-TWG Head

Approved: / Disapproved:

JAIME CASTO JOSE P. GARCHITORENA
President and CEO/OIC, CIMS

Bidder's/Supplier's Conforme

_____
Signature over Printed Name

_____
Capacity

Duly authorized to sign for and on behalf of:_____