Republic of the Philippines
DEPARTMENT OF FINANCE
Roxas Blvd. corner P. Ocampo St., 1004 Manila

BAGONG PILIPINAS

REQUEST FOR QUOTATION

RFQ No.: 2024-05-0065
Date : May 22, 2024

____
____
____

Gentlemen :

Please quote your lowest price on the item listed below, subject to the General Conditions at the back hereof and submit your quotation duly signed by your representative in sealed envelope direct to the Bids and Awards Committee (BAC) Chairperson or through the authorized canvasser of this Department not later than ______________________ the time and date of the opening of the sealed quotation.

ALVIN P. DIAZ
Director IV
Central Administration Office

QUANTITY	UNIT	ARTICLE / MERCHANDISE / SPECIFICATION	UNIT PRICE	TOTAL
1	Lot	**SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF CYBER RISK RATING PLATFORM** *SEE ATTACHED TERMS OF REFERENCE*	1,000,000.000	1,000,000.00
		NOTE: Please include the following required documents upon submission of your proposal for evaluation purposes: **1. Mayor's/Business Permit** **2. PhilGEPS Registration Number** **3. Latest Income/Business Tax Return** Additional required document to be submitted by the winning bidder upon issuance of the Job Order: **4. Duly notarized Omnibus Sworn Statement**		
TOTAL AMOUNT				**₱1,000,000.00**

After having carefully read and accepted the general conditions, I/we quote you on the item at prices noted above and bind ourselves to deliver the above articles/merchandise within 30 calendar days from receipt of your valid Purchase Order (PO). The quotation are good only up to 60 calendar days.

Canvassed by:

____

Supplier : ______________________________
By : ______________________________
Tel. No.: ______________________________
TIN : ______________________________

Republic of the Philippines
DEPARTMENT OF FINANCE
Roxas Blvd. corner P. Ocampo St., 1004 Manila

BAGONG PILIPINAS

REQUEST FOR QUOTATION

RFQ No.: 2024-05-0065
Date : ___________

____
____
____

Gentlemen :

Please quote your lowest price on the item listed below, subject to the General Conditions at the back hereof and submit your quotation duly signed by your representative in sealed envelope direct to the Bids and Awards Committee (BAC) Chairperson or through the authorized canvasser of this Department not later than ________________________ the time and date of the opening of the sealed quotation.

ALVIN P. DIAZ
Director IV
Central Administration Office

QUANTITY	UNIT	ARTICLE / MERCHANDISE / SPECIFICATION	UNIT PRICE	TOTAL
1	Lot	**SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF CYBER RISK RATING PLATFORM** *SEE ATTACHED TERMS OF REFERENCE*		
		NOTE: Please include the following required documents upon submission of your proposal for evaluation purposes: **1. Mayor's/Business Permit** **2. PhilGEPS Registration Number** **3. Latest Income/Business Tax Return** Additional required document to be submitted by the winning bidder upon issuance of the Job Order: **4. Duly notarized Omnibus Sworn Statement**		
TOTAL AMOUNT				

After having carefully read and accepted the general conditions, I/we quote you on the item at prices noted above and bind ourselves to deliver the above articles/merchandise within 30 calendar days from receipt of your valid Purchase Order (PO). The quotation are good only up to 60 calendar days.

Canvassed by:

____

Supplier : ________________________________
By : ________________________________
Tel. No.: ________________________________
TIN : ________________________________

GENERAL CONDITIONS

1. The bidders are required to submit brochures, literatures, pictures and technical data pertaining to the brand and model of the equipment being offered.

2. The quotation will not be considered unless it is properly signed by the bidder's authorized representative.

3. All prizes quoted herein are valid and binding for a period of sixty (60) days.

4. Bidder shall be responsible for the source of his equipment.

5. Subject to the provisions of the preceeding paragraph, where awardee has accepted a Purchase Order (PO) but fails to deliver the required products within the time called for in the same order, he must return the order accompanied by written explanations within the period of delivery of the merchandise. Thereafter, if the awardee has not completed delivery within the period, the subject PO shall be cancelled and the award shall be withdrawn from that supplier. The DOF shall then purchase the required item from such other sources as it may determine, with the price difference to be charged against the defaulting awardee.

6. The DOF reserves the right to reject any or all quotations, to waive any formality therein or to accept such quotations as may be considered most advantageous to the government.

TECHNICAL SPECIFICATIONS

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF THE CYBER RISK RATING PLATFORM
RFQ No. 2024-05-0065 dated May 22, 2024

I. PROJECT SCOPE

The winning bidder must supply and deliver:

Item	Description	Qty	Total Amount *(VAT inclusive)*
1	Supply, Delivery, Installation and Configuration of the Cyber Risk Rating Platform	1 Lot	₱1,000,000.00

II. TECHNICAL SPECIFICATIONS

Detailed Minimum Specifications of the Items to be Procured

a. ***Software License:*** Must be able to provide a cyber risk rating platform that includes self-monitoring for eight (8) slot license package
b. ***Support and Subscription:*** One (1) year
c. ***Documentation:*** Shall provide document manual as well as test report of the implemented platform

GENERAL

- □ The proposed solution must have at least 10 years of providing Cyber Risk Ratings solution and/or services.
- □ The proposed solution must be recognized for its performance and customer service by top industry analysts and publications.
- □ The proposed solution must have accreditations such as SOC Type 2 for services.
- □ The proposed solution and/or services should be named as a technology leader in a reputable 3rd party research / advisory company.

MULTI-FACTOR AUTHENTICATION

- □ The proposed solution and/or services should support multi-factor authentication for the sign in process.

PLATFORM

- □ The proposed solution and/or services should be a SaaS platform.
- □ The proposed solution and/or services should not require installation of any software such as agents, clients; and/or hardware of any type, in the environment of the organization and third-parties organization to be monitored.
- □ The proposed solution and/or services has a service uptime commitment of 98% or more during the term of the subscription

DATA TRANSPARENCY/ACCURACY

- □ The proposed solution and/or services should be a signatory of Principles for Fair and Accurate Security Ratings from reputed business federations and associations.
- □ The proposed solution and/or services must allow and has a process for rated organizations to challenge their rating and provide corrected or clarifying data.
- □ The proposed solution and/or services should publish the following information in public:
  - ○ Refute Rate and Refute Response Time
  - ○ IP Misattribution - Refute Rate and Domain Misattribution - Refute Rate

□ The proposed solution and/or services must be able to provide white paper on their Data Collection, Data Attribution and Scoring Methodology.

□ The proposed solution and/or services must be able to provide white paper on the correlation of security ratings (scores) with relative likelihood of breach

CYBERSECURITY RISK RATINGS

Continuous Monitoring

1.1 The proposed solution and/or services must be able to continuously monitoring at least 8 domains with cybersecurity risk ratings

1.2 The proposed solution and/or services must be able to provide a cybersecurity risk ratings platform that enables the DOF to assess and manage its own cybersecurity posture. The cybersecurity risk ratings platform should have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.

1.3 The proposed solution and/or services must be able to provide a cybersecurity risk ratings platform that enables them to assess and manage the third-party vendors / business partners. The cybersecurity risk ratings platform should have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.

1.4 The proposed solution and/or services must be able to allow benchmark of the DOF's cybersecurity posture against industry peers, competitors, or other organizations

Benchmark

1.5 The proposed solution and/or services must be able to benchmark the DOF and/or other bureaus and attached agencies potential security issues that has been detected, against one of the several recognized information security frameworks available, not limited to:

1.5.1 ISO/IEC 27001:2022
1.5.2 NIST CSF
1.5.3 SOC2

1.6 The proposed solution and/or services must be able to support showcase of DOF's compliance evidence, browse compliance evidence for any organization, or request evidence from an organization.

Risk Factor

1.7 The proposed solution and/or services must be able to support data collection and should include but not limited to the following risk factors:

1.7.1 Network Security
1.7.2 DNS Health
1.7.3 Patching Cadence
1.7.4 Endpoint Security
1.7.5 IP Reputation
1.7.6 Application Security
1.7.7 Cubit Score
1.7.8 Hacker Chatter
1.7.9 Information Leak
1.7.10 Social Engineering

1.8 The proposed solution and/or services must be able to provide a simple rating system to come up with a clear and easy-to-understand view of an organization's cybersecurity posture.

Provisional Scorecard

1.9 The proposed solution and/or services must be able to generate an initial score for a company new to the cybersecurity risk ratings platform in minutes rather than hours or days.

Portfolio / Group

1.10 The proposed solution and/or services must be able to allow the DOF to self-service, to organize portfolios in groups to assess their overall risk and align with specific project or role.

Custom Scorecard

1.11 The proposed solution and/or services must be able to allow the DOF to self-service to have granular visibility into the risk posture of its individual business units, subsidiaries, and other types of organizational structures by building its own custom scope for cybersecurity risk ratings and get a detailed rating on-demand.

Digital Footprint

1.12 The proposed solution and/or services must be able to create a Digital Footprint of the DOF's internet-facing assets as it collects and analyses cybersecurity signals and calculates the cyber risk rating.

1.13 The proposed solution and/or services must be able to provide a visualization of all the assets that have been attributed to DOF, organized by IP addresses, IP ranges, domains, and geographic distribution.

1.14 The proposed solution and/or services has a detection method and must include but not limited to the following:

1.14.1 DNS Lookup
1.14.2 Port Scan
1.14.3 Published Data
1.14.4 User Input
1.14.5 Platform Login
1.14.6 Third-Party
1.14.7 WHOIS

1.15 The proposed solution and/or services must be able to allow the DOF to self-validate their Digital Footprints via review, claim, manage and add assets.

1.16 For managing assets, the proposed solution and/or services must be able to review the DOF submitted request within 72 hours. The ratings score should be updated within approximately 48 hours after approval.

History / Event Log

1.17 The proposed solution and/or services must be able to provide transparency into score changes with a historical score chart.

1.18 The proposed solution and/or services must be able to provide the historical score chart, and should be able to view historical score changes of the last 7 days, 30 days, 6 months, 12 months, or YTD.

1.19 The proposed solution and/or services must have an event log that provides further transparency around score fluctuations with a clear record of issue changes and their impact on overall grade.

1.20 The Event Log should cover the following:

1.20.1 New Findings: Newly detected findings for issues added

1.20.2 Resolved Findings: Findings for issues the company resolved internally

1.20.3 Decayed Findings: Findings for issues that no longer impact the score

1.20.4 Security Events: Breaches, Incidents, etc.

Issues / Score Planner

1.21 The proposed solution and/or services must allow to build or automatically generate a plan to improve DOF's score while providing full transparency into how specific security issues impact.

Alert

1.22 The proposed solution and/or services must enable the DOF to automate monitoring for score changes based on numerical thresholds and grade drops and raises and receive notifications in-app and via email.

Report

1.23 The proposed solution and/or services must be able to generate, view, and share reports from the cybersecurity risk ratings platform.

1.24 The proposed solution and/or services must be able to generate at least three types of reports (Summary, Issues, or Detailed Report)

1.25 The proposed solution and/or services must be able to schedule future sending of a generated report.

QUESTIONNAIRE

1.1 The proposed solution and/or services must be able to provide an automated questionnaire and evidence exchange platform that automatically provides insight into the validity of questionnaire responses.

1.2 The proposed solution and/or services must have an automated questionnaire and evidence exchange platform should support the following:

1.2.1 Questionnaire: Upload or create a custom questionnaire template or choose from a list of industry standard template questionnaires.

1.2.2 Send: Send a questionnaire to one vendor or multiple vendors at once. With options to send once or recurring schedules

1.2.3 Track: Track the status of every questionnaire, see due dates, and see turnaround time of all the questionnaires. Supports automatic reminders.

1.2.4 Validate: Once a questionnaire is done, there should be email notification and the questionnaire and attachments can be reviewed. The engine of this platform should map cybersecurity risk ratings to individual responses, allowing the agency/organization to trust and verify questionnaire responses.

INTEGRATION

1.1 The proposed solution and/or services must have integration with leading Integrated Risk Management, Third Party Risk Management, and/or Vulnerability Management vendors.

1.2 The proposed solution and/or services must have at least 90 technology and integration partners

API

1.1 The proposed solution and/or services should make an available API service

1.2 The proposed solution and/or services has a documentation for the API service.

CUSTOMER SUCCESS

1.1 Should assign a designated Customer Success Manager within Asia for the subscription period.
1.2 Customer Success Manager should conduct a quarterly review session with the DOF.
1.3 The quarterly review session should be conducted onsite at DOF office

ONBOARDING

1.1 The assigned Customer Success Manager should be the single point of contact for the onboarding.
1.2 The assigned Customer Success Manager should provide a timeline for the onboarding and describe the onboarding process.
1.3 Must conduct operational training / portal walk through at the end of the onboarding.

TRAINING/EDUCATION

1.1 Must conduct/provide training of the proposed solution for at least 3 CMIO personnel.

- □ The winning BIDDER/SUPPLIER shall provide installation, best practice configuration, operational and maintenance training of the proposed Cyber Risk Rating Platform
- □ The training shall be conducted at a designated venue and shall be attended by at least three (3) CMIO personnel.
- □ The winning BIDDER/SUPPLIER shall provide all training resources including but not limited to training modules, handouts and certificates.

1.2 Must have the capability to conduct / provide third party risk management related certification courses.
1.3 Must conduct/ provide at least three (3) Third Party Risk Management related certification courses

V. SCHEDULE OF REQUIREMENTS

The delivery schedule stipulates hereafter the delivery date, which is the actual date of delivery to the project site:

No.	Description	Delivery Schedule
1	Cyber Risk Rating Platform ***Eight (8) slot license package for one (1) year***	30CD upon receipt of the PO
2	Documentation	
3	Training	

VI. PAYMENT TERMS

Full payment upon complete delivery and acceptance of the solution

VII. CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

Shall follow the DOF Confidentiality and Non-Disclosure Agreement

I hereby certify to comply and deliver all the above requirements.

____

Signature over Printed Name of the Representative
Company Name : ______________________
Date Signed : ______________________
Email/Phone No.: ______________________

TECHNICAL SPECIFICATIONS

SUPPLY, DELIVERY, INSTALLATION AND CONFIGURATION OF THE CYBER RISK RATING PLATFORM
RFQ No. 2024-05-0065 dated May 22, 2024

I. PROJECT SCOPE

The winning bidder must supply and deliver:

Item	Description	Qty	Total Amount *(VAT inclusive)*
1	Supply, Delivery, Installation and Configuration of the Cyber Risk Rating Platform	1 Lot	₱1,000,000.00

II. TECHNICAL SPECIFICATIONS

Detailed Minimum Specifications of the Items to be Procured

a. ***Software License:*** Must be able to provide a cyber risk rating platform that includes self-monitoring for eight (8) slot license package
b. ***Support and Subscription:*** One (1) year
c. ***Documentation:*** Shall provide document manual as well as test report of the implemented platform

GENERAL

- □ The proposed solution must have at least 10 years of providing Cyber Risk Ratings solution and/or services.
- □ The proposed solution must be recognized for its performance and customer service by top industry analysts and publications.
- □ The proposed solution must have accreditations such as SOC Type 2 for services.
- □ The proposed solution and/or services should be named as a technology leader in a reputable 3rd party research / advisory company.

MULTI-FACTOR AUTHENTICATION

- □ The proposed solution and/or services should support multi-factor authentication for the sign in process.

PLATFORM

- □ The proposed solution and/or services should be a SaaS platform.
- □ The proposed solution and/or services should not require installation of any software such as agents, clients; and/or hardware of any type, in the environment of the organization and third-parties organization to be monitored.
- □ The proposed solution and/or services has a service uptime commitment of 98% or more during the term of the subscription

DATA TRANSPARENCY/ACCURACY

- □ The proposed solution and/or services should be a signatory of Principles for Fair and Accurate Security Ratings from reputed business federations and associations.
- □ The proposed solution and/or services must allow and has a process for rated organizations to challenge their rating and provide corrected or clarifying data.
- □ The proposed solution and/or services should publish the following information in public:
  - ○ Refute Rate and Refute Response Time
  - ○ IP Misattribution - Refute Rate and Domain Misattribution - Refute Rate

□ The proposed solution and/or services must be able to provide white paper on their Data Collection, Data Attribution and Scoring Methodology.

□ The proposed solution and/or services must be able to provide white paper on the correlation of security ratings (scores) with relative likelihood of breach

CYBERSECURITY RISK RATINGS

Continuous Monitoring

1.1 The proposed solution and/or services must be able to continuously monitoring at least 8 domains with cybersecurity risk ratings

1.2 The proposed solution and/or services must be able to provide a cybersecurity risk ratings platform that enables the DOF to assess and manage its own cybersecurity posture. The cybersecurity risk ratings platform should have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.

1.3 The proposed solution and/or services must be able to provide a cybersecurity risk ratings platform that enables them to assess and manage the third-party vendors / business partners. The cybersecurity risk ratings platform should have the ability to generate risk ratings, identify security gaps, and provide remediation guidance.

1.4 The proposed solution and/or services must be able to allow benchmark of the DOF's cybersecurity posture against industry peers, competitors, or other organizations

Benchmark

1.5 The proposed solution and/or services must be able to benchmark the DOF and/or other bureaus and attached agencies potential security issues that has been detected, against one of the several recognized information security frameworks available, not limited to:

1.5.1 ISO/IEC 27001:2022
1.5.2 NIST CSF
1.5.3 SOC2

1.6 The proposed solution and/or services must be able to support showcase of DOF's compliance evidence, browse compliance evidence for any organization, or request evidence from an organization.

Risk Factor

1.7 The proposed solution and/or services must be able to support data collection and should include but not limited to the following risk factors:

1.7.1 Network Security
1.7.2 DNS Health
1.7.3 Patching Cadence
1.7.4 Endpoint Security
1.7.5 IP Reputation
1.7.6 Application Security
1.7.7 Cubit Score
1.7.8 Hacker Chatter
1.7.9 Information Leak
1.7.10 Social Engineering

1.8 The proposed solution and/or services must be able to provide a simple rating system to come up with a clear and easy-to-understand view of an organization's cybersecurity posture.

Provisional Scorecard

1.9 The proposed solution and/or services must be able to generate an initial score for a company new to the cybersecurity risk ratings platform in minutes rather than hours or days.

Portfolio / Group

1.10 The proposed solution and/or services must be able to allow the DOF to self-service, to organize portfolios in groups to assess their overall risk and align with specific project or role.

Custom Scorecard

1.11 The proposed solution and/or services must be able to allow the DOF to self-service to have granular visibility into the risk posture of its individual business units, subsidiaries, and other types of organizational structures by building its own custom scope for cybersecurity risk ratings and get a detailed rating on-demand.

Digital Footprint

1.12 The proposed solution and/or services must be able to create a Digital Footprint of the DOF's internet-facing assets as it collects and analyses cybersecurity signals and calculates the cyber risk rating.

1.13 The proposed solution and/or services must be able to provide a visualization of all the assets that have been attributed to DOF, organized by IP addresses, IP ranges, domains, and geographic distribution.

1.14 The proposed solution and/or services has a detection method and must include but not limited to the following:

1.14.1 DNS Lookup
1.14.2 Port Scan
1.14.3 Published Data
1.14.4 User Input
1.14.5 Platform Login
1.14.6 Third-Party
1.14.7 WHOIS

1.15 The proposed solution and/or services must be able to allow the DOF to self-validate their Digital Footprints via review, claim, manage and add assets.

1.16 For managing assets, the proposed solution and/or services must be able to review the DOF submitted request within 72 hours. The ratings score should be updated within approximately 48 hours after approval.

History / Event Log

1.17 The proposed solution and/or services must be able to provide transparency into score changes with a historical score chart.

1.18 The proposed solution and/or services must be able to provide the historical score chart, and should be able to view historical score changes of the last 7 days, 30 days, 6 months, 12 months, or YTD.

1.19 The proposed solution and/or services must have an event log that provides further transparency around score fluctuations with a clear record of issue changes and their impact on overall grade.

1.20 The Event Log should cover the following:

1.20.1 New Findings: Newly detected findings for issues added

1.20.2 Resolved Findings: Findings for issues the company resolved internally

1.20.3 Decayed Findings: Findings for issues that no longer impact the score

1.20.4 Security Events: Breaches, Incidents, etc.

Issues / Score Planner

1.21 The proposed solution and/or services must allow to build or automatically generate a plan to improve DOF's score while providing full transparency into how specific security issues impact.

Alert

1.22 The proposed solution and/or services must enable the DOF to automate monitoring for score changes based on numerical thresholds and grade drops and raises and receive notifications in-app and via email.

Report

1.23 The proposed solution and/or services must be able to generate, view, and share reports from the cybersecurity risk ratings platform.

1.24 The proposed solution and/or services must be able to generate at least three types of reports (Summary, Issues, or Detailed Report)

1.25 The proposed solution and/or services must be able to schedule future sending of a generated report.

QUESTIONNAIRE

1.1 The proposed solution and/or services must be able to provide an automated questionnaire and evidence exchange platform that automatically provides insight into the validity of questionnaire responses.

1.2 The proposed solution and/or services must have an automated questionnaire and evidence exchange platform should support the following:

1.2.1 Questionnaire: Upload or create a custom questionnaire template or choose from a list of industry standard template questionnaires.

1.2.2 Send: Send a questionnaire to one vendor or multiple vendors at once. With options to send once or recurring schedules

1.2.3 Track: Track the status of every questionnaire, see due dates, and see turnaround time of all the questionnaires. Supports automatic reminders.

1.2.4 Validate: Once a questionnaire is done, there should be email notification and the questionnaire and attachments can be reviewed. The engine of this platform should map cybersecurity risk ratings to individual responses, allowing the agency/organization to trust and verify questionnaire responses.

INTEGRATION

1.1 The proposed solution and/or services must have integration with leading Integrated Risk Management, Third Party Risk Management, and/or Vulnerability Management vendors.

1.2 The proposed solution and/or services must have at least 90 technology and integration partners

API

1.1 The proposed solution and/or services should make an available API service

1.2 The proposed solution and/or services has a documentation for the API service.

CUSTOMER SUCCESS

1.1 Should assign a designated Customer Success Manager within Asia for the subscription period.

1.2 Customer Success Manager should conduct a quarterly review session with the DOF.

1.3 The quarterly review session should be conducted onsite at DOF office

ONBOARDING

1.1 The assigned Customer Success Manager should be the single point of contact for the onboarding.

1.2 The assigned Customer Success Manager should provide a timeline for the onboarding and describe the onboarding process.

1.3 Must conduct operational training / portal walk through at the end of the onboarding.

TRAINING/EDUCATION

1.1 Must conduct/provide training of the proposed solution for at least 3 CMIO personnel.

□ The winning BIDDER/SUPPLIER shall provide installation, best practice configuration, operational and maintenance training of the proposed Cyber Risk Rating Platform

□ The training shall be conducted at a designated venue and shall be attended by at least three (3) CMIO personnel.

□ The winning BIDDER/SUPPLIER shall provide all training resources including but not limited to training modules, handouts and certificates.

1.2 Must have the capability to conduct / provide third party risk management related certification courses.

1.3 Must conduct/ provide at least three (3) Third Party Risk Management related certification courses

V. SCHEDULE OF REQUIREMENTS

The delivery schedule stipulates hereafter the delivery date, which is the actual date of delivery to the project site:

No.	Description	Delivery Schedule
1	Cyber Risk Rating Platform ***Eight (8) slot license package for one (1) year***	30CD upon receipt of the PO
2	Documentation	
3	Training	

VI. PAYMENT TERMS

Full payment upon complete delivery and acceptance of the solution

VII. CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

Shall follow the DOF Confidentiality and Non-Disclosure Agreement

I hereby certify to comply and deliver all the above requirements.

____

Signature over Printed Name of the Representative

Company Name : ____________________________

Date Signed : ____________________________

Email/Phone No.: ____________________________