Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue
Manila

**BIDS AND AWARDS COMMITTEE**

**SUPPLEMENTAL BID BULLETIN NO. 2**

**Conduct of Third-Party Vulnerability Assessment and Penetration Testing for the Insurance Commission (Project Reference No. 2023–11–359)**

This Supplemental Bid Bulletin No. 2, dated 14 December 2023, is being issued to clarify, modify, or amend items in the Bidding Document.

The following item in the Bidding Document for the **Conduct of Third-Party Vulnerability Assessment and Penetration Testing for the Insurance Commission** dated 25 November 2023 is hereby revised/amended:

1. Amendment of **Section III (Bid Data Sheet) ITB Clause 5.3 and 20.2** are hereby amended as follows:

   **FROM:**

| ITB Clause | |
|---|---|
| 5.3 | For this purpose, contracts similar to the Project shall be:<br><br>**a. Conduct of Third-Party Vulnerability Assessment and Penetration Testing for the Insurance Commission**<br><br>b. Completed within Five (5) years prior to the deadline for the submission and receipt of bids. |
| 20.2 | e. Brochure (original or internet download/Technical Data Sheet or equivalent) of the following items/services being offered showing compliance to the technical specifications attached with its corresponding computation. (If not in English, please refer to Clause 10.3 of the Instructions to Bidders and Section 23.2 of the 2016 Revised IRR of RA 9184):<br>i. **Conduct of Third-Party Vulnerability Assessment and Penetration Testing for the Insurance Commission *(In case of Joint Venture, both partners must present/submit items a and b)*** |

**TO:**

| ITB Clause | |
|---|---|
| 5.3 | For this purpose, contracts similar to the Project shall be:<br><br>**a. Conduct of Third-Party Vulnerability Assessment and Penetration Testing**<br><br>b. Completed within Five (5) years prior to the deadline for the submission and receipt of bids. |
| 20.2 | e. Brochure (original or internet download/Technical Data Sheet or equivalent) of the following items/services being offered showing compliance to the technical specifications attached with its corresponding computation. (If not in English, please refer to Clause 10.3 of the Instructions to Bidders and Section 23.2 of the 2016 Revised IRR of RA 9184):<br>i. **Conduct of Third-Party Vulnerability Assessment and Penetration Testing *(In case of Joint Venture, both partners must present/submit items a and b)*** |

2. Amendment of **Section VI (Schedule of Requirements) Item 2** is hereby amended as follows:

**FROM:**

2. **Service Level Agreement/Warranty Certificate**

**The winning bidder must submit an implementation Schedule indicating the required activities and the date of implementation, Sales/Service Invoice, and Service Level Agreement (SLA)/Warranty Certificate.**

**TO:**

2. **Service Level Agreement/Warranty Certificate**

**The winning bidder must submit an Implementation Schedule indicating the required activities and the date of implementation within the fifteen (15) calendar days from the receipt of Notice to Proceed, and Sales/Service Invoice.**

**The IC shall engage with the actual VAPT activities of the Service Provider for an estimated period of forty-five (45) calendar days, from 8:00PM to 6:00AM only, excluding remediation period of the IC.**

3. Amendment of **Section VII (Technical Specifications)** is hereby amended as follows:

**FROM:**

## IC EXTERNAL VULNERABILITY ASSESSMENT AND PENETRATION TESTING

### 1. Objectives and Goals

Objective: To evaluate the overall security posture of the IC public-facing systems.

Goals: Identify and assess vulnerabilities, validate the effectiveness of existing security controls, and enhance the overall security posture of the Insurance Commission to protect sensitive customer data and maintain regulatory compliance.

### 2. In-Scope Systems

Public-facing systems in scope include:
Website: www.insurance.gov.ph
API: Prod and Staging servers (will be disclosed after NDA)
Web Applications: 7 mission critical app servers (will be disclosed after NDA)

### 3. Out-of-Scope Systems

- Phishing/Social Engineering attack against any IC employees or its customers
- Physical attacks against IC facilities/IT infrastructure
- Destructive actions or Denial of Service (DoS) attacks
- Modifications to the environment without written consent from the IC VAPT Team Lead

### 4. Testing Methodology

Black-box testing applying guides, methodologies, and frameworks, prescribed by NIST, OSSTMM, CIS, PTES, and OWASP-WSTG.

### 5. Legal and Compliance Considerations

The testing must comply with all relevant legal and regulatory requirements.

### 6. Timing and Schedule

A kickoff meeting will be held before the engagement period to ensure a smooth start and discussion of the period and schedule.

## 7. Testing Scenarios

Automated and manual unauthenticated analysis of the external web applications, vulnerability threat vectorization, verification, and exploitation.

## 8. Reporting and Deliverables

A. The final report will include an executive summary, detailed findings, risk assessments, and recommendations in a PDF format.

B. Detailed findings must include identification tests, attack chain walkthrough, and results of tests performed including the ff
   - Tools used and methodology employed
   - List of vulnerabilities identified
   - Description of vulnerability
   - Risk rating or severity of vulnerability
   - Category of Risk: Very High(Critical) / High / Medium / Low
   - CVSS 3.1 Score computation and CWE
   - Security Impact
   - Actual exploitation of vulnerabilities (Proof on Concept)
   - Commands use in the attack chain

## 9. Remediation Guidelines

The VAPT team must provide detailed guidance on how to address vulnerabilities discovered, including references to relevant security best practices and resources.

## 10. Communication and Escalation

- Primary point of contact & IC VAPT Team Lead: Engr. Jason M. Ampoloquio
- Issues should be reported within 24 hours of discovery and escalated if not resolved within 7 days.

## 11. Confidentiality and Data Protection

- All sensitive data accessed during testing will be handled securely and deleted after the assessment.
- All offensive activities, scripts, implants, webshells, or any payloads used during engagement must be documented and deleted after the testing.

## 12. Documentation and Sign-off

Both the organization and VAPT team will sign a formal agreement that outlines the scope and terms of the engagement.

## 13. Budget and Resources

A budget of Php2,000,000.00 is allocated for this VAPT project.

## 14. Pentester Requirements

The VAPT Pen testers must hold at least 2 of the ff certifications.

- OSCP
- GPEN
- Pentest+
- OSEP
- OSWE
- CRTO
- CPTS
- CBBH

**TO:**

# IC EXTERNAL VULNERABILITY ASSESSMENT AND PENETRATION TESTING

## 1. Objectives and Goals

Objective: To evaluate the overall security posture of the IC public-facing systems.

Goals: Identify and assess vulnerabilities, validate the effectiveness of existing security controls, and enhance the overall security posture of the Insurance Commission to protect sensitive customer data and maintain regulatory compliance.

## 2. In-Scope Systems

- **Public-facing systems in scope include:**
  - **Website: www.insurance.gov.ph**
  - **API: Prod and Staging servers (will be disclosed after NDA)**
  - **Web Applications: 7 mission critical application servers (will be disclosed after NDA)**

- **Privilege escalation is allowed solely for the designated system and is prohibited from extending or utilizing such privileges beyond the specified scope or within the internal network of the IC.**

## 3. Out-of-Scope Systems

- Phishing/Social Engineering attack against any IC employees or its customers

- Physical attacks against IC facilities/IT infrastructure
- Destructive actions or Denial of Service (DoS) attacks
- Modifications to the environment without written consent from the IC VAPT Team Lead
- **IC Internal Network and other systems, applications, and devices outside the in-scope items**

4. **Testing Methodology**

   Black-box testing applying guides, methodologies, and frameworks, prescribed by NIST, OSSTMM, CIS, PTES, OWASP-WSTG, **and ISMS 20071**.

5. **Legal and Compliance Considerations**

   The testing must comply with all relevant legal and regulatory requirements.

6. **Timing and Schedule**

   **The winning bidder must submit an Implementation Schedule indicating the required activities and the date of implementation within the fifteen (15) calendar days from the receipt of Notice to Proceed, and Sales/Service Invoice.**

   **A kickoff meeting will be held before the engagement period to ensure a smooth start and discussion of the period and schedule.**

   **The IC shall engage with the actual VAPT activities of the Service Provider for an estimated period of forty-five (45) calendar days, from 8:00PM to 6:00AM only, excluding remediation period of the IC.**

7. **Testing Scenarios**

   Automated and manual unauthenticated analysis of the external web applications, vulnerability threat vectorization, verification, and exploitation.

8. **Reporting and Deliverables**

   A. The final report will include an executive summary, detailed findings, risk assessments, and recommendations in a PDF format.

   B. Detailed findings must include identification tests, attack chain walkthrough, and results of tests performed including the ff
      - Tools used and methodology employed
      - List of vulnerabilities identified
      - Description of vulnerability
      - Risk rating or severity of vulnerability
      - Category of Risk: Very High(Critical) / High / Medium / Low

- CVSS 3.1 Score computation and CWE
- Security Impact
- Actual exploitation of vulnerabilities (Proof on Concept)
- Commands use in the attack chain

## 9. Remediation Guidelines

The VAPT team must provide detailed guidance on how to address vulnerabilities discovered, including references to relevant security best practices and resources.

## 10. Communication and Escalation

- Primary point of contact & IC VAPT Team Lead: Engr. Jason M. Ampoloquio
- **Issues encountered during the actual VAPT activities (i.e. system- and service-related issues, denial of service, security patch conflicts, data loss, etc.) should be reported within 24 hours of discovery and escalated if not resolved within 7 days.**

## 11. Confidentiality and Data Protection

- All sensitive data accessed during testing will be handled securely and deleted after the assessment.
- All offensive activities, scripts, implants, webshells, or any payloads used during engagement must be documented and deleted after the testing.

## 12. Documentation and Sign-off

Both the organization and VAPT team will sign a formal agreement that outlines the scope and terms of the engagement.

## 13. Budget and Resources

A budget of Php2,000,000.00 is allocated for this VAPT project.

## 14. Pentester Requirements

**Each VAPT Pentester/s must hold at least any two (2) of the following certifications:**

- OSCP
- GPEN
- Pentest+
- OSEP
- OSWE
- CRTO
- CPTS
- CBBH

- **OSCE³**
- **eLearnSecurity Junior Penetration Tester**
- **eLearnSecurity Certified Professional Penetration Tester**
- **Pentester Academy Certified Red Team Professional**

4. Amendment of **Section VIII (Checklist of Technical Documents) Item I. TECHNICAL COMPONENT ENVELOPE** is hereby amended as follows:

   **FROM:**

   (c) Statement of the bidder's Single Largest Completed Contract (SLCC) similar nature within the last five (5) years from the date of submission and receipt of bids equivalent to at least fifty (50%) of the total ABC (per IC Form No. 4); and

   Similar in Nature shall mean **"Conduct of Third-Party Vulnerability Assessment and Penetration Testing for the Insurance Commission"**

   **TO:**

   (c) Statement of the bidder's Single Largest Completed Contract (SLCC) similar nature within the last five (5) years from the date of submission and receipt of bids equivalent to at least fifty (50%) of the total ABC (per IC Form No. 4); and

   Similar in Nature shall mean **"Conduct of Third-Party Vulnerability Assessment and Penetration Testing"**

This Supplemental Bid Bulletin No. 2 shall form part of the Bid Documents. Any provisions in the Bid Documents inconsistent herewith are hereby amended, modified, and superseded accordingly.

For the information and guidance of all concerned.

Issued this 14 December 2023 in the City of Manila.

[ORIGINAL SIGNED]
**MR. ARTURO S. TRINIDAD II**
BAC Chairperson
Bids and Awards Committee

Supplemental Bid Bulletin No. 2 for the ***Conduct of Third-Party Vulnerability Assessment and Penetration Testing for the Insurance Commission (Project Reference No. 2023–11–359)*** dated 14 December 2023 consisting of nine (9) pages.

Received by:

Name of the Bidder/Company: _____

Name of Authorized Representative/s: _____

Signature/s: _____