Republic of the Philippines
Department of Social Welfare and Development
IBP Road, Constitution Hills, Quezon City
Telephone Nos. (02) 931-8101 to 07 Local 122/123/124
Email Address: bacsec@dswd.gov.ph

BIDDING DOCUMENTS

SUBSCRIPTION TO MANAGED SERVICES FOR DSWD COMPLETE SUITE OF PRIMARY ICT SECURITY DEVICES

ITB No. GOP/20-DSWD-060
(PR No. 2020090143)

NOVEMBER 2020

PHILIPPINE BIDDING DOCUMENTS

(As Harmonized with Development Partners)

Procurement of GOODS

Government of the Republic of the Philippines

Sixth Edition
July 2020

Table of Contents

Glossary of Acronyms, Terms, and Abbreviations

ABC – Approved Budget for the Contract.

BAC – Bids and Awards Committee.

Bid – A signed offer or proposal to undertake a contract submitted by a bidder in response to and in consonance with the requirements of the bidding documents. Also referred to as *Proposal* and *Tender*. (2016 revised IRR, Section 5[c])

Bidder – Refers to a contractor, manufacturer, supplier, distributor and/or consultant who submits a bid in response to the requirements of the Bidding Documents. (2016 revised IRR, Section 5[d])

Bidding Documents – The documents issued by the Procuring Entity as the bases for bids, furnishing all information necessary for a prospective bidder to prepare a bid for the Goods, Infrastructure Projects, and/or Consulting Services required by the Procuring Entity. (2016 revised IRR, Section 5[e])

BIR – Bureau of Internal Revenue.

BSP – Bangko Sentral ng Pilipinas.

Consulting Services – Refer to services for Infrastructure Projects and other types of projects or activities of the GOP requiring adequate external technical and professional expertise that are beyond the capability and/or capacity of the GOP to undertake such as, but not limited to: (i) advisory and review services; (ii) pre-investment or feasibility studies; (iii) design; (iv) construction supervision; (v) management and related services; and (vi) other technical services or special studies. (2016 revised IRR, Section 5[i])

CDA - Cooperative Development Authority.

Contract – Refers to the agreement entered into between the Procuring Entity and the Supplier or Manufacturer or Distributor or Service Provider for procurement of Goods and Services; Contractor for Procurement of Infrastructure Projects; or Consultant or Consulting Firm for Procurement of Consulting Services; as the case may be, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

CIF – Cost Insurance and Freight.

CIP – Carriage and Insurance Paid.

CPI – Consumer Price Index.

DDP – Refers to the quoted price of the Goods, which means "delivered duty paid."

DTI – Department of Trade and Industry.

EXW – Ex works.

FCA – "Free Carrier" shipping point.

FOB – "Free on Board" shipping point.

Foreign-funded Procurement or Foreign-Assisted Project– Refers to procurement whose funding source is from a foreign government, foreign or international financing institution as specified in the Treaty or International or Executive Agreement. (2016 revised IRR, Section 5[b]).

Framework Agreement – Refers to a written agreement between a procuring entity and a supplier or service provider that identifies the terms and conditions, under which specific purchases, otherwise known as "Call-Offs," are made for the duration of the agreement. It is in the nature of an option contract between the procuring entity and the bidder(s) granting the procuring entity the option to either place an order for any of the goods or services identified in the Framework Agreement List or not buy at all, within a minimum period of one (1) year to a maximum period of three (3) years. (GPPB Resolution No. 27-2019)

GFI – Government Financial Institution.

GOCC – Government-owned and/or –controlled corporation.

Goods – Refer to all items, supplies, materials and general support services, except Consulting Services and Infrastructure Projects, which may be needed in the transaction of public businesses or in the pursuit of any government undertaking, project or activity, whether in the nature of equipment, furniture, stationery, materials for construction, or personal property of any kind, including non-personal or contractual services such as the repair and maintenance of equipment and furniture, as well as trucking, hauling, janitorial, security, and related or analogous services, as well as procurement of materials and supplies provided by the Procuring Entity for such services. The term "related" or "analogous services" shall include, but is not limited to, lease or purchase of office space, media advertisements, health maintenance services, and other services essential to the operation of the Procuring Entity. (2016 revised IRR, Section 5[r])

GOP – Government of the Philippines.

GPPB – Government Procurement Policy Board.

INCOTERMS – International Commercial Terms.

Infrastructure Projects – Include the construction, improvement, rehabilitation, demolition, repair, restoration or maintenance of roads and bridges, railways, airports, seaports, communication facilities, civil works components of information technology projects, irrigation, flood control and drainage, water supply, sanitation, sewerage and solid waste management systems, shore protection, energy/power and electrification facilities, national

buildings, school buildings, hospital buildings, and other related construction projects of the government. Also referred to as *civil works or works*. (2016 revised IRR, Section 5[u])

LGUs – Local Government Units.

NFCC – Net Financial Contracting Capacity.

NGA – National Government Agency.

PhilGEPS - Philippine Government Electronic Procurement System.

Procurement Project – refers to a specific or identified procurement covering goods, infrastructure project or consulting services. A Procurement Project shall be described, detailed, and scheduled in the Project Procurement Management Plan prepared by the agency which shall be consolidated in the procuring entity's Annual Procurement Plan. (GPPB Circular No. 06-2019 dated 17 July 2019)

PSA – Philippine Statistics Authority.

SEC – Securities and Exchange Commission.

SLCC – Single Largest Completed Contract.

Supplier – refers to a citizen, or any corporate body or commercial company duly organized and registered under the laws where it is established, habitually established in business and engaged in the manufacture or sale of the merchandise or performance of the general services covered by his bid. (Item 3.8 of GPPB Resolution No. 13-2019, dated 23 May 2019). Supplier as used in these Bidding Documents may likewise refer to a distributor, manufacturer, contractor, or consultant.

UN – United Nations.

Section I. Invitation to Bid

INVITATION TO BID FOR

SUBSCRIPTION TO MANAGED SERVICES FOR DSWD COMPLETE SUITE OF PRIMARY ICT SECURITY DEVICES

— ITB NO. GOP/20-DSWD-060 —

(PR NO. 2020090143)

1. The **Department of Social Welfare and Development (DSWD)**, through the **Information and Communications Technology Management Service (ICTMS) – Maintenance and Other Operating Expenses (MOOE) 2021 National Expenditure Program (NEP)** intends to apply the sum of **Forty-Two Million Pesos (PHP 42,000,000.00)** being the ABC to payments under the contract for **Subscription to Managed Services for DSWD Complete Suite of Primary ICT Security Devices.** Bids received in excess of the ABC shall be automatically rejected at bid opening.

2. The DSWD now invites bids for the above Procurement Project. Delivery of the Goods and/or Services shall be in accordance with Section VI (Schedule of Requirements). Bidders should have completed, within **five (5) years** from the date of submission and receipt of bids, a contract similar to the Project. The description of an eligible bidder is contained in the Bidding Documents, particularly, in Section II (Instructions to Bidders).

3. Bidding will be conducted through open competitive bidding procedures using a non-discretionary "*pass/fail*" criterion as specified in the 2016 revised Implementing Rules and Regulations (IRR) of Republic Act (RA) No. 9184.

   Bidding is restricted to Filipino citizens/sole proprietorships, partnerships, or organizations with at least sixty percent (60%) interest or outstanding capital stock belonging to citizens of the Philippines, and to citizens or organizations of a country the laws or regulations of which grant similar rights or privileges to Filipino citizens, pursuant to RA No. 5183.

4. Prospective Bidders may obtain further information from **DSWD BAC Secretariat** and inspect the Bidding Documents at the address given below during **08:00 AM** to **05:00 PM** from **Monday** to **Friday**.

5. A complete set of Bidding Documents may be acquired by interested Bidders on **25 November 2020** to **14 December 2020** from the given address and website(s) below and upon payment of the applicable fee for the Bidding Documents in the amount of **Twenty-Five Thousand Pesos (PHP 25,000.00)**.

It may also be downloaded free of charge from the website of the PhilGEPS and the website of the Procuring Entity, provided that Bidders shall pay the applicable fee for the Bidding Documents not later than the submission of their bids.

6. The DSWD will hold a Pre-Bid Conference on **02 December 2020, 02:30 PM** at **Katapatan Conference Room (Boardroom), 4/F Magiliw Building, DSWD Central Office, IBP Road, Constitution Hills, Quezon City** and/or through video conferencing or webcasting **via google meet**, which shall be open to prospective bidders.

7. Bids must be duly received by the BAC Secretariat through manual submission at the office address indicated below, on or before **14 December 2020, 12:00 PM**. Late bids shall not be accepted.

8. All Bids must be accompanied by a bid security in any of the acceptable forms and in the amount stated in **ITB** Clause 14.

9. Bid opening shall be on **14 December 2020, 02:30 PM** at the **Agency Operations Center, 1/F Mahusay Building, DSWD Central Office, IBP Road, Constitution Hills, Quezon City**. Bids will be opened in the presence of the bidders' representatives who choose to attend the activity.

10. To facilitate the immediate implementation of the procurement of this Project, the DSWD shall proceed with the conduct of Early Procurement Activities (EPA), pursuant to Section 7.6 of the 2016 Revised IRR of RA 9184, Section 19 of the General Provisions of the FY 2021 NEP and Government Procurement Policy Board (GPPB) Resolution No. 14-2019 dated 17 July 2019.

11. The DSWD reserves the right to reject any and all bids, declare a failure of bidding, or not award the contract at any time prior to contract award in accordance with Sections 35.6 and 41 of the 2016 revised IRR of RA No. 9184, without thereby incurring any liability to the affected bidder or bidders.

12. For further information, please refer to:

THE CHAIRPERSON
DSWD Bids and Awards Committee
c/o BAC Secretariat
2nd Floor, Mahusay Building, DSWD Central Office
IBP Road, Constitution Hills, Quezon City
Email Address: bacsec@dswd.gov.ph
Telephone Nos.: (02) 931-8101 to 07 Locals 122/123/124
Fax No.: (02) 951-7116

13. You may visit the following websites:

For downloading of Bidding Documents: www.philgeps.gov.ph or www.dswd.gov.ph

24 November 2020

(Original Signed)
RENE GLEN O. PAJE
Undersecretary and
Chairperson, Bids and Awards Committee

Section II. Instructions to Bidders

1. Scope of Bid

The Procuring Entity, **DSWD** wishes to receive Bids for the **Subscription to Managed Services for DSWD Complete Suite of Primary ICT Security Devices**, with identification number **ITB No. GOP/20-DSWD-060**.

The Procurement Project (referred to herein as "Project") is composed of **one (1) lot**, the details of which are described in Section VII (Technical Specifications).

2. Funding Information

2.1. The GOP through the source of funding as indicated below for **2021 NEP** in the amount of **Forty-Two Million Pesos (PHP 42,000,000.00)**.

2.2. The source of funding is:

a. NGA, the National Expenditure Program.

3. Bidding Requirements

The Bidding for the Project shall be governed by all the provisions of RA No. 9184 and its 2016 revised IRR, including its Generic Procurement Manuals and associated policies, rules and regulations as the primary source thereof, while the herein clauses shall serve as the secondary source thereof.

Any amendments made to the IRR and other GPPB issuances shall be applicable only to the ongoing posting, advertisement, or **IB** by the BAC through the issuance of a supplemental or bid bulletin.

The Bidder, by the act of submitting its Bid, shall be deemed to have verified and accepted the general requirements of this Project, including other factors that may affect the cost, duration and execution or implementation of the contract, project, or work and examine all instructions, forms, terms, and project requirements in the Bidding Documents.

4. Corrupt, Fraudulent, Collusive, and Coercive Practices

The Procuring Entity, as well as the Bidders and Suppliers, shall observe the highest standard of ethics during the procurement and execution of the contract. They or through an agent shall not engage in corrupt, fraudulent, collusive, coercive, and obstructive practices defined under Annex "I" of the 2016 revised IRR of RA No. 9184 or other integrity violations in competing for the Project.

5. Eligible Bidders

5.1. Only Bids of Bidders found to be legally, technically, and financially capable will be evaluated.

5.2. Foreign ownership exceeding those allowed under the rules may participate pursuant to:

i. When a Treaty or International or Executive Agreement as provided in Section 4 of the RA No. 9184 and its 2016 revised IRR allow foreign bidders to participate;

ii. Citizens, corporations, or associations of a country, included in the list issued by the GPPB, the laws or regulations of which grant reciprocal rights or privileges to citizens, corporations, or associations of the Philippines;

iii. When the Goods sought to be procured are not available from local suppliers; or

iv. When there is a need to prevent situations that defeat competition or restrain trade.

5.3. Pursuant to Section 23.4.1.3 of the 2016 revised IRR of RA No.9184, the Bidder shall have an SLCC that is at least one (1) contract similar to the Project the value of which, adjusted to current prices using the PSA's CPI, must be at least equivalent to:

a. For the procurement of Non-expendable Supplies and Services: The Bidder must have completed a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC.

5.4. The Bidders shall comply with the eligibility criteria under Section 23.4.1 of the 2016 IRR of RA No. 9184.

6. Origin of Goods

There is no restriction on the origin of goods other than those prohibited by a decision of the UN Security Council taken under Chapter VII of the Charter of the UN, subject to Domestic Preference requirements under **ITB** Clause 18.

7. Subcontracts

7.1. The Bidder may subcontract portions of the Project to the extent allowed by the Procuring Entity as stated herein, but in no case more than twenty percent (20%) of the Project.

The Procuring Entity has prescribed that:

a. Subcontracting is not allowed.

7.2. Subcontracting of any portion of the Project does not relieve the Supplier of any liability or obligation under the Contract. The Supplier will be responsible for the acts, defaults, and negligence of any subcontractor, its agents, servants, or workmen as fully as if these were the Supplier's own acts, defaults, or negligence, or those of its agents, servants, or workmen.

8. Pre-Bid Conference

The Procuring Entity will hold a pre-bid conference for this Project on the specified date and time and either at its physical address and/or through videoconferencing/webcasting as indicated in paragraph 6 of the **IB.**

9. Clarification and Amendment of Bidding Documents

Prospective bidders may request for clarification on and/or interpretation of any part of the Bidding Documents. Such requests must be in writing and received by the Procuring Entity, either at its given address or through electronic mail indicated in the **IB**, at least ten (10) calendar days before the deadline set for the submission and receipt of Bids.

10. Documents comprising the Bid: Eligibility and Technical Components

10.1. The first envelope shall contain the eligibility and technical documents of the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.

10.2. The Bidder's SLCC as indicated in **ITB** Clause 5.3 should have been completed within **five (5) years** prior to the deadline for the submission and receipt of bids.

10.3. If the eligibility requirements or statements, the bids, and all other documents for submission to the BAC are in foreign language other than English, it must be accompanied by a translation in English, which shall be authenticated by the appropriate Philippine foreign service establishment, post, or the equivalent office having jurisdiction over the foreign bidder's affairs in the Philippines. Similar to the required authentication above, for Contracting Parties to the Apostille Convention, only the translated documents shall be authenticated through an apostille pursuant to GPPB Resolution No. 13-2019 dated 23 May 2019. The English translation shall govern, for purposes of interpretation of the bid.

11. Documents comprising the Bid: Financial Component

11.1. The second bid envelope shall contain the financial documents for the Bid as specified in **Section VIII (Checklist of Technical and Financial Documents)**.

11.2. If the Bidder claims preference as a Domestic Bidder or Domestic Entity, a certification issued by DTI shall be provided by the Bidder in accordance with Section 43.1.3 of the 2016 revised IRR of RA No. 9184.

11.3. Any bid exceeding the ABC indicated in paragraph 1 of the **IB** shall not be accepted.

11.4. For Foreign-funded Procurement, a ceiling may be applied to bid prices provided the conditions are met under Section 31.2 of the 2016 revised IRR of RA No. 9184.

12. Bid Prices

12.1. Prices indicated on the Price Schedule shall be entered separately in the following manner:

a. For Goods offered from within the Procuring Entity's country:

i. The price of the Goods quoted EXW (ex-works, ex-factory, ex-warehouse, ex-showroom, or off-the-shelf, as applicable);

ii. The cost of all customs duties and sales and other taxes already paid or payable;

iii. The cost of transportation, insurance, and other costs incidental to delivery of the Goods to their final destination; and

iv. The price of other (incidental) services, if any, listed in e.

b. For Goods offered from abroad:

i. Unless otherwise stated in the **BDS**, the price of the Goods shall be quoted delivered duty paid (DDP) with the place of destination in the Philippines as specified in the **BDS**. In quoting the price, the Bidder shall be free to use transportation through carriers registered in any eligible country. Similarly, the Bidder may obtain insurance services from any eligible source country.

ii. The price of other (incidental) services, if any, as listed in **Section VII (Technical Specifications).**

13. Bid and Payment Currencies

13.1. For Goods that the Bidder will supply from outside the Philippines, the bid prices may be quoted in the local currency or tradeable currency accepted by the BSP at the discretion of the Bidder. However, for purposes of bid evaluation, Bids denominated in foreign currencies, shall be converted to Philippine currency based on the exchange rate as published in the BSP reference rate bulletin on the day of the bid opening.

13.2. Payment of the contract price shall be made in:

a. Philippine Pesos.

14. Bid Security

14.1. The Bidder shall submit a Bid Securing Declaration or any form of Bid Security in the amount indicated in the **BDS**, which shall be not less than the percentage of the ABC in accordance with the schedule in the **BDS**.

14.2. The Bid and bid security shall be valid until **One Hundred Twenty (120) calendar days from the date of opening of bids**. Any Bid not accompanied

by an acceptable bid security shall be rejected by the Procuring Entity as non-responsive.

15. Sealing and Marking of Bids

Each Bidder shall submit one copy of the first and second components of its Bid.

The Procuring Entity may request additional hard copies and/or electronic copies of the Bid. However, failure of the Bidders to comply with the said request shall not be a ground for disqualification.

If the Procuring Entity allows the submission of bids through online submission or any other electronic means, the Bidder shall submit an electronic copy of its Bid, which must be digitally signed. An electronic copy that cannot be opened or is corrupted shall be considered non-responsive and, thus, automatically disqualified.

16. Deadline for Submission of Bids

16.1. The Bidders shall submit on the specified date and time and either at its physical address or through online submission as indicated in paragraph 7 of the **IB.**

17. Opening and Preliminary Examination of Bids

17.1. The BAC shall open the Bids in public at the time, on the date, and at the place specified in paragraph 9 of the **IB**. The Bidders' representatives who are present shall sign a register evidencing their attendance. In case videoconferencing, webcasting or other similar technologies will be used, attendance of participants shall likewise be recorded by the BAC Secretariat.

In case the Bids cannot be opened as scheduled due to justifiable reasons, the rescheduling requirements under Section 29 of the 2016 revised IRR of RA No. 9184 shall prevail.

17.2. The preliminary examination of bids shall be governed by Section 30 of the 2016 revised IRR of RA No. 9184.

18. Domestic Preference

18.1. The Procuring Entity will grant a margin of preference for the purpose of comparison of Bids in accordance with Section 43.1.2 of the 2016 revised IRR of RA No. 9184.

19. Detailed Evaluation and Comparison of Bids

19.1. The Procuring BAC shall immediately conduct a detailed evaluation of all Bids rated "*passed*," using non-discretionary pass/fail criteria. The BAC shall consider the conditions in the evaluation of Bids under Section 32.2 of the 2016 revised IRR of RA No. 9184.

19.2. If the Project allows partial bids, bidders may submit a proposal on any of the lots or items, and evaluation will be undertaken on a per lot or item basis, as the case maybe. In this case, the Bid Security as required by **ITB** Clause 15 shall be submitted for each lot or item separately.

19.3. The descriptions of the lots or items shall be indicated in **Section VII (Technical Specifications)**, although the ABCs of these lots or items are indicated in the **BDS** for purposes of the NFCC computation pursuant to Section 23.4.2.6 of the 2016 revised IRR of RA No. 9184. The NFCC must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder.

19.4. The Project shall be awarded as follows:

Option 1 – One Project having several items that shall be awarded as one contract.

19.5. Except for bidders submitting a committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation, all Bids must include the NFCC computation pursuant to Section 23.4.1.4 of the 2016 revised IRR of RA No. 9184, which must be sufficient for the total of the ABCs for all the lots or items participated in by the prospective Bidder. For bidders submitting the committed Line of Credit, it must be at least equal to ten percent (10%) of the ABCs for all the lots or items participated in by the prospective Bidder.

20. Post-Qualification

20.1. Within a non-extendible period of five (5) calendar days from receipt by the Bidder of the notice from the BAC that it submitted the Lowest Calculated Bid, the Bidder shall submit its latest income and business tax returns filed and paid through the BIR Electronic Filing and Payment System (eFPS) and other appropriate licenses and permits required by law and stated in the **BDS**.

21. Signing of the Contract

21.1. The documents required in Section 37.2 of the 2016 revised IRR of RA No. 9184 shall form part of the Contract. Additional Contract documents are indicated in the **BDS**.

Section III. Bid Data Sheet

Bid Data Sheet

<table>
<tr><th>ITB Clause</th><th></th></tr>
<tr><td>5.3</td><td>For this purpose, contracts similar to the Project shall be:

a. subscription to ICT security devices or firewalls.

b. completed within five (5) years prior to the deadline for the submission and receipt of bids.</td></tr>
<tr><td>7.1</td><td>Subcontracting is not allowed.</td></tr>
<tr><td>12</td><td>The price of the Goods shall be quoted DDP at the delivery site indicated in Section VI (Schedule of Requirements) or the applicable International Commercial Terms (INCOTERMS) for this Project.</td></tr>
<tr><td>14.1</td><td>The bid security shall be in the form of a Bid Securing Declaration, or any of the following forms and amounts:

a. The amount of not less than PHP 840,000.00 if bid security is in cash, cashier’s/manager’s check, bank draft/guarantee or irrevocable letter of credit; or

b. The amount of not less than PHP 2,100,000.00 if bid security is in Surety Bond.</td></tr>
<tr><td>15</td><td>Each Bidder shall submit one (1) original and one (1) copy of the first and second components of its Bid. Forms provided in Section IX (Bidding Forms) must be completed without any alterations to their format, and no substitute form shall be accepted.</td></tr>
<tr><td>19.3</td><td><table><tr><th>Particulars</th><th>Quantity</th><th>ABC
(in PHP)</th></tr><tr><td>Subscription to Managed Services for DSWD Complete Suite of Primary ICT Security Devices</td><td>1 lot</td><td>42,000,000.00</td></tr></table></td></tr>
<tr><td>20.2</td><td>The Lowest Calculated Bid (LCB) or Single Calculated Bid (SCB) as the case may be, shall submit the following additional documents during the Post-Qualification Stage:

1) Latest income tax returns (ITR) are those covering the immediately preceding year while latest business tax returns (BTR) are those filed within the last six (6) months preceding the date of bid submission;

2) Updated Certificate of PhilGEPS Registration (Platinum Membership);</td></tr>
</table>

	3) Original and duly notarized certification from the Service Provider that they have been in the ICT business for the last ten (10) years; 4) Original and duly notarized certification from the Service Provider that they have at least five (5) years' experience and expertise in providing professional service such as manage services, maintenance support, on-call trouble shooting, consulting, training and migration services; 5) Original and duly notarized certification from the Service Provider that the offered solution/ goods has been in the market for at least five (5) years; 6) List of clients in Luzon, Visayas, Mindanao and the National Capital Region (NCR) (at least one in each area) which the service provider had previously deployed the solution/ goods successfully; 7) Original and duly notarized certification from the Service Provider that they would allow transition period of at least three (3) months beyond the last contract month to prevent service interruption while the successor project is being implemented; and, 8) Certification that the offered solutions has passed the laboratory testing from International Computer Security Association (ICSA) Labs or NSS Labs or CSfC, ANSSI or equivalent; and,
21.2	The Lowest Calculated and Responsive Bid (LCRB) or Single Calculated and Responsive Bid (SCRB) who opted to submit Surety Bond as form of Performance Security shall submit a certification from the Insurance Commission (IC) indicating the following details: 1) The Certification was issued in favor of an insurance/ bonding company; and, 2) The insurance/ bonding company is authorized to issue bonds/ sureties in favor of the supplier/ service provider for the said project.

Section IV. General Conditions of Contract

1. Scope of Contract

This Contract shall include all such items, although not specifically mentioned, that can be reasonably inferred as being required for its completion as if such items were expressly mentioned herein. All the provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, constitute the primary source for the terms and conditions of the Contract, and thus, applicable in contract implementation. Herein clauses shall serve as the secondary source for the terms and conditions of the Contract.

This is without prejudice to Sections 74.1 and 74.2 of the 2016 revised IRR of RA No. 9184 allowing the GPPB to amend the IRR, which shall be applied to all procurement activities, the advertisement, posting, or invitation of which were issued after the effectivity of the said amendment.

Additional requirements for the completion of this Contract shall be provided in the **Special Conditions of Contract** (**SCC).**

2. Advance Payment and Terms of Payment

2.1. Advance payment of the contract amount is provided under Annex "D" of the revised 2016 IRR of RA No. 9184.

2.2. The Procuring Entity is allowed to determine the terms of payment on the partial or staggered delivery of the Goods procured, provided such partial payment shall correspond to the value of the goods delivered and accepted in accordance with prevailing accounting and auditing rules and regulations. The terms of payment are indicated in the **SCC**.

3. Performance Security

Within ten (10) calendar days from receipt of the Notice of Award by the Bidder from the Procuring Entity but in no case later than prior to the signing of the Contract by both parties, the successful Bidder shall furnish the performance security in any of the forms prescribed in Section 39 of the 2016 revised IRR of RA No. 9184.

4. Inspection and Tests

The Procuring Entity or its representative shall have the right to inspect and/or to test the Goods to confirm their conformity to the Project specifications at no extra cost to the Procuring Entity in accordance with the Generic Procurement Manual. In addition to tests in the **SCC**, **Section IV (Technical Specifications)** shall specify what inspections and/or tests the Procuring Entity requires, and where they are to be conducted. The Procuring Entity shall notify the Supplier in writing, in a timely manner, of the identity of any representatives retained for these purposes.

All reasonable facilities and assistance for the inspection and testing of Goods, including access to drawings and production data, shall be provided by the Supplier to the authorized inspectors at no charge to the Procuring Entity.

5. Warranty

5.1. In order to assure that manufacturing defects shall be corrected by the Supplier, a warranty shall be required from the Supplier as provided under Section 62.1 of the 2016 revised IRR of RA No. 9184.

5.2. The Procuring Entity shall promptly notify the Supplier in writing of any claims arising under this warranty. Upon receipt of such notice, the Supplier shall, repair or replace the defective Goods or parts thereof without cost to the Procuring Entity, pursuant to the Generic Procurement Manual.

6. Liability of the Supplier

The Supplier's liability under this Contract shall be as provided by the laws of the Republic of the Philippines.

If the Supplier is a joint venture, all partners to the joint venture shall be jointly and severally liable to the Procuring Entity.

Section V. Special Conditions of Contract

Special Conditions of Contract

GCC Clause	
1	**Delivery and Documents –** For purposes of the Contract, "EXW," "FOB," "FCA," "CIF," "CIP," "DDP" and other trade terms used to describe the obligations of the parties shall have the meanings assigned to them by the current edition of INCOTERMS published by the International Chamber of Commerce, Paris. The Delivery terms of this Contract shall be as follows: *For Goods supplied from abroad:* The delivery terms applicable to the Contract are DDP delivered as indicated in Section VI (Schedule of Requirements). In accordance with INCOTERMS. *For Goods supplied from within the Philippines:* The delivery terms applicable to this Contract are as indicated in Section VI (Schedule of Requirements). Risk and title will pass from the Supplier to the Procuring Entity upon receipt and final acceptance of the Goods at their final destination. Delivery of the Goods shall be made by the Supplier in accordance with the terms specified in Section VI (Schedule of Requirements). For purposes of this Clause the Procuring Entity's Representative at the Project Site is defined in Section VI (Schedule of Requirements).
	Incidental Services – The Supplier is required to provide all additional services, if any, specified in Section VI. Schedule of Requirements. The Contract price for the Goods shall include the prices charged by the Supplier for incidental services and shall not exceed the prevailing rates charged to other parties by the Supplier for similar services.
	Spare Parts – The Supplier is required to provide all of the materials, notifications, and information pertaining to spare parts manufactured or distributed by the Supplier: a. such spare parts as the Procuring Entity may elect to purchase from the Supplier, provided that this election shall not relieve the Supplier of any warranty obligations under this Contract; and b. in the event of termination of production of the spare parts:

	i. advance notification to the Procuring Entity of the pending termination, in sufficient time to permit the Procuring Entity to procure needed requirements; and ii. following such termination, furnishing at no cost to the Procuring Entity, the blueprints, drawings, and specifications of the spare parts, if requested. The spare parts and other components required, if any, are listed in Section VI (Schedule of Requirements) and the cost thereof are included in the contract price.
	Packaging – The Supplier shall provide such packaging of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in this Contract. The packaging shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packaging case size and weights shall take into consideration, where appropriate, the remoteness of the Goods' final destination and the absence of heavy handling facilities at all points in transit. The packaging, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified below, and in any subsequent instructions ordered by the Procuring Entity. The outer packaging must be clearly marked on at least four (4) sides as follows: Name of the Procuring Entity Name of the Supplier Contract Description Final Destination Gross weight Any special lifting instructions Any special handling instructions Any relevant HAZCHEM classifications A packaging list identifying the contents and quantities of the package is to be placed on an accessible point of the outer packaging if practical. If not practical the packaging list is to be placed inside the outer packaging but outside the secondary packaging.
	Transportation – Where the Supplier is required under Contract to deliver the Goods CIF, CIP, or DDP, transport of the Goods to the port of destination or such other named place of destination in the Philippines, as shall be specified in this Contract,

	shall be arranged and paid for by the Supplier, and the cost thereof shall be included in the Contract Price. Where the Supplier is required under this Contract to transport the Goods to a specified place of destination within the Philippines, defined as the Project Site, transport to such place of destination in the Philippines, including insurance and storage, as shall be specified in this Contract, shall be arranged by the Supplier, and related costs shall be included in the contract price. Where the Supplier is required under Contract to deliver the Goods CIF, CIP or DDP, Goods are to be transported on carriers of Philippine registry. In the event that no carrier of Philippine registry is available, Goods may be shipped by a carrier which is not of Philippine registry provided that the Supplier obtains and presents to the Procuring Entity certification to this effect from the nearest Philippine consulate to the port of dispatch. In the event that carriers of Philippine registry are available but their schedule delays the Supplier in its performance of this Contract the period from when the Goods were first ready for shipment and the actual date of shipment the period of delay will be considered force majeure. The Procuring Entity accepts no liability for the damage of Goods during transit other than those prescribed by INCOTERMS for DDP deliveries. In the case of Goods supplied from within the Philippines or supplied by domestic Suppliers risk and title will not be deemed to have passed to the Procuring Entity until their receipt and final acceptance at the final destination.
	Intellectual Property Rights – The Supplier shall indemnify the Procuring Entity against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the Goods or any part thereof.
2.2	The terms of payment shall be in accordance with Section VI (Schedule of Requirements).
4	The DSWD-Inspection Committee, in cooperation with the Information and Communication Technology Management Service (ICTMS) and Procurement Management Service (PMS), shall inspect the goods/services and conduct tests for the compliance with the required technical specifications prior to deployment.

Section VI. Schedule of Requirements

Particulars	Quantity
A. Central Office	
• 10G Next Generation Firewall for CO Wide Area Network (WAN)	• 2 units (HA mode)
• Next Generation Firewall for Local Area Network (LAN)	• 2 units (HA mode)
• 10G Next Generation IPS for CO	• 2 units (1 sensor, 1 Management Console)
• FW Centralize Management	• 1 unit (Admin Management for all Firewall)
B. Field Offices	
• 10G Next Generation Firewall	• 17 units (16 FOs, 1 spare)
C. Disaster Recovery Site	
• Next Generation Firewall for DR	• 2 units (HA mode)
• 10G Next Generation IPS for DR	• 1 Sensor Unit

A. Delivery Sites*

1. Central Office – DSWD Complex, Batasan Hills, Quezon City
2. Disaster Recovery Site – Clark Pampanga (whichever is the active DR Site of DSWD for the year)
3. 16 Field Offices
   a. DSWD Field Office 1 – San Fernando City, La Union
   b. DSWD Field Office 2 – Carig, Sur, Tuguegarao City
   c. DSWD Field Office 3 – San Fernando City, Pampanga
   d. DSWD Field Office 4A – Muntinlupa City
   e. DSWD Field Office 4B – Malate, Manila
   f. DSWD Field Office 5 – Legaspi City, Albay
   g. DSWD Field Office 6 – Molo, Iloilo
   h. DSWD Field Office 7 – Cebu
   i. DSWD Field Office 8 – Tacloban City, Leyte
   j. DSWD Field Office 9 – Zamboanga,Del Sur
   k. DSWD Field Office 10 – Misamis Oriental, CDO
   l. DSWD Field Office 11 – Davao Del Sur
   m. DSWD Field Office 12 – Koronadal City, South Cotabato
   n. DSWD Field Office CARAGA – Butuan City, Agusan Del Norte
   o. DSWD Field Office CAR – Baguio City, Benguet
   p. DSWD Field Office NCR – Legarda, Manila

**In coordination with the ICTMS*

B. Coverage:

- Implementation: Ninety (90) calendar days for all components
- Maintenance and Support Coverage: until 31 December 2021

C. Project Phases, Deliverables and Terms of Payment

Milestone	Project Phases	Expected Deliverables	Completion Indicators	Payment (% of the Total Contract Prices)
1	Kick-off and Inception (15 calendar days after NTP)	• Kick-off documentation and Inception Report • Approved Implementation Plan	• Submitted Kick-off documents and both Party Agreements • Submitted Inception Reports • Submitted and Approved Implementation Plan	10%
2	Supply and Delivery of Firewall Devices and IPS Devices (60 calendar days after NTP)	• Delivery of Firewall and IPS equipment to all locations • Acceptance Report	• Complete Delivery Receipts	40%
3	Configuration, Testing and Acceptance (90 calendar days after NTP)	• Setup and Configuration • Successful Testing and Turn-over	• Complete Documentation • User's Acceptance	25%
4	Management, Monitoring and Maintenance Support Checkpoint (180 days after NTP)	• Consolidation of Monthly Operation Report • Summary of Interventions and issue resolutions provided • Training Vouchers or Training Certificate	• Certificate of Satisfactory Service Completion	25%

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

Section VII. Technical Specifications

Technical Specifications

DSWD Specifications	Bidder's Specifications[1]
I. NEXT GENERATION UNIFIED THREAT MANAGEMENT **A. CENTRAL OFFICE (CO) REQUIREMENT** **1. Next Generation Unified Threat Management for Wide Area Network** 1.1. Functional Requirements *Platform* 1.1.1. The Service Provider shall propose two (2) 10G Next Generation Firewalls with a capability of supporting at least fifteen (15) gigabit per second of application firewall throughput and at least eight (8) gigabit per second for threat prevention and modern malware protection. 1.1.2. The proposed firewalls shall support at least three (3) million concurrent sessions and at least ONE HUNDRED AND FIFTY THOUSAND (150,000) new sessions per second. 1.1.3. The proposed firewalls shall support at least FIVE THOUSAND (5,000) concurrent sessions of SSL VPN clients inclusive of any required subscription licenses. 1.1.4. Each of the proposed firewalls should have a provision of at least TWENTY	Brand: Model: Detailed Specifications:

[1] *IMPORTANT NOTE: Detailed Specifications must be provided. Bidders must state here either "Comply" or "Not Comply" against each of the individual parameters of each Specification stating the corresponding performance parameter of the equipment offered. Statements of "Comply" or "Not Comply" must be supported by evidence in a Bidders Bid and cross-referenced to that evidence. Evidence shall be in the form of manufacturer's un-amended sales literature, unconditional statements of specification and compliance issued by the manufacturer, samples, independent test data etc., as appropriate. A statement that is not supported by evidence or is subsequently found to be contradicted by the evidence presented will render the Bid under evaluation liable for rejection. A statement either in the Bidder's statement of compliance or the supporting evidence that is found to be false either during Bid evaluation, post-qualification or the execution of the Contract may be regarded as fraudulent and render the Bidder or supplier liable for prosecution subject to the applicable laws and issuances.*

	(20) 10G network ports inclusive of at least SIXTEEN (16) SFP/SPF+ transceivers that are necessary to establish complete connectivity with existing network devices in the location.	
1.1.5.	The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console.	
1.1.6.	The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture.	
1.1.7.	The proposed firewalls shall be administered centrally by **the same brand used for central management of all the firewalls** to ensure full compatibility and optimized configuration.	
1.1.8.	The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware.	

1.1.9. The proposed firewall must have a capability to provide **secure portalized access to Intranet Web Applications** without the need to install a VPN Client. 1.1.10. Proposed firewall must be configured with **HIGH AVAILABILITY.** 1.1.11. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI or equivalent). 1.2. Please see additional feature specifications on **ANNEX "A".** **2. Next Generation Unified Threat Management for CO Local Area Network** 2.1. Functional Requirement *Platform* 2.1.1. The Service Provider shall propose two (2) Next 10G Generation Firewall (inclusive of 1 on-site spare) with the capability of supporting at least FIVE (5) gigabit per second of application firewall throughput and TWO (2) gigabit per second for threat prevention and modern malware protection. 2.1.2. The proposed firewalls shall support at least ONE (1) million concurrent sessions and at least SEVENTY THOUSAND (70, 000) new sessions per second. 2.1.3. Each of the proposed firewalls should have at least FOUR (4) gigabit network ports and FOUR (4) 10G network ports inclusive of at least FOUR (4) SFP/SPF+ transceivers that are necessary to establish complete connectivity with existing network devices in the location	

2.1.4. The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console. 2.1.5. The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture. 2.1.6. The proposed firewalls shall be administered centrally by the same brand used for central management of all the firewalls. 2.1.7. The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware. 2.1.8. Proposed firewall must be configured with **HIGH AVAILABILITY**. 2.1.9. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI or equivalent).	

2.2. Please see additional feature specifications on **ANNEX "A".** **3. Next Generation Firewall Centralized Management Platform for CO** 3.1. Feature Specifications *Platform* 3.1.1. The Service Provider shall propose ONE (1) Next Generation Firewall Centralized Management Appliance with a capability of supporting at least TWENTY FIVE (25) remote firewalls. 3.1.2. The proposed Centralized Firewall Management must be capable of both PASSIVE and ACTIVE high availability setup. 3.1.3. The proposed Centralized Firewall Management must be capable of both Local and RADIUS administrator's authentication. 3.1.4. The proposed Centralized Firewall Management must have GUI, Command Line Interface XML-Based REST API for management console. 3.1.5. The proposed Centralized Firewall Management must be capable of supporting RAID with at least 16TB usable capacity. 3.1.6. The proposed Centralized Firewall Management must be have redundant power supply. 3.2. Please see additional feature specifications on **ANNEX "A".** **B. FIELD OFFICES (FO) REQUIREMENT** **1. Next Generation Unified Threat Management Device for Field Offices** 1.1. Functional Requirements	

Platform 1.1.1. The Service Provider shall propose SIXTEEN (16) 10G Next Generation Firewalls (proposed firewalls) with one (1) spare with a capability of supporting at least TWO (2) gigabits per second of application firewall throughput and at least SEVEN HUNDRED FIFTY (750) megabit per second for threat prevention and modern malware protection. 1.1.2. The proposed firewalls shall support at least ONE HUNDRED FIFTY THOUSAND (150,000) concurrent sessions and at least TEN THOUSAND (10,000) new sessions per second. 1.1.3. Each of the proposed firewalls should have at least FOUR (4) gigabit network ports and FOUR (4) 10G network ports inclusive of at least SIXTEEN (16) SFP/SPF+ transceivers that are necessary to establish complete connectivity with existing network devices in the location. 1.1.4. The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console. 1.1.5. The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle	

signature matching and processing in a single pass parallel processing architecture. 1.1.6. The proposed firewalls shall be administered centrally on the central management appliance using the same brand. 1.1.7. The proposed firewall shall have modern malware protection that identifies unknown malicious files by directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware. 1.1.8. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI or equivalent). 1.2. Please see additional feature specifications on **ANNEX "A".** **C. DISASTER RECOVERY SITE: REMOTE DATACENTER** **1. Next Generation Unified Threat Management Device for DR Site** 1.1. Functional Requirements *Platform* 1.1.1. The Service Provider shall propose TWO (2) 10G Next Generation Firewalls (inclusive of on-site spare) with the capability of supporting at least FIVE (5) GIGABIT per second of application firewall throughput and at least TWO (2) GIGABIT per second for threat prevention and modern malware protection. 1.1.2. The proposed firewalls shall support at least ONE MILLION (1,000,000)	

concurrent sessions and at least ONE HUNDRED TWENTY THOUSAND (120,000) new sessions per second. 1.1.3. The proposed firewalls shall support at least FIVE THOUSAND (5,000) concurrent sessions of SSL VPN clients inclusive of any required subscription licenses. 1.1.4. The proposed firewalls should have at least TWENTY (20) 10G network ports inclusive of at least sixteen (16) SFP/SPF+ transceivers that are necessary to establish complete connectivity with existing network devices in the location. 1.1.5. The proposed firewalls must allow policy rule creation for application identification, user identification, threat prevention, Uniform Resource Locator (URL) filtering, traffic management Quality of Service (QoS) per policy and scheduling in a single unified rule and not in multiple data-entry locations in the management console. 1.1.6. The proposed firewalls shall have the hardened Operating System (OS) and built as a firewall appliance (i.e. not on generic server hardware) and shall handle traffic in a stream-based manner with all features turned on. It shall be optimized for layer 7 application level content processing and have special Application-Specific Integrated Circuit (ASIC) to handle signature matching and processing in a single pass parallel processing architecture. 1.1.7. The proposed firewalls shall be administered centrally similar to the central office and field offices using the central management solution. 1.1.8. The proposed firewall shall have modern malware protection that identifies unknown malicious files by	

directly and automatically executing them in a virtual cloud-based environment to expose malicious behavior even if the malware has never been seen in the wild before without the need for additional hardware. 1.1.9. The proposed firewalls must have passed and been certified by third party evaluations (e.g. NSS Labs, ICSA Labs, CSfC, ANSSI or equivalent). 1.1.10. Proposed firewall must be configured with **HIGH AVAILABILITY**. 1.2. Please see additional feature specifications on **ANNEX "A".** **II. Next Generation Intrusion Prevention System (IPS) for DSWD** **1. Central Office Requirement:** 1.1. Sensors: 1.1.1. Appliance with at least 18x (9 in-line pairs) 10G ports capable of at least 10Gbps inspection throughput. 1.1.2. In-line port pairs must support traffic-bypass in cases of device failure. 1.1.3. Must connect to the IPS Management System. 1.2. Management Center: 1.2.1. Appliance purposely built for management of IPS Sensors described above. 1.3. Please see additional feature specifications on **ANNEX "B".** **2. Remote Datacenter Requirement:** 2.1. Sensors:	

2.1.1. Appliance with at least 18x (9 in-line pairs 10G ports capable of 10Gbps inspection throughput.

2.1.2. In-line port pairs must support traffic-bypass in cases of device failure.

2.1.3. Must connect to the Management System located at Central Office.

2.2. Please see additional feature specifications on **ANNEX "B".**

III. Project Coverage

A. Service Area

The **service provider** will be reporting to the DSWD offices if there are major issues or concerns that need resolution.

1. Central Office - DSWD Complex, Batasan Hills, Quezon City

2. DR Site – (whichever is the active DR Site of DSWD for the year)

3. 16 Field Offices

Field Office	Site
1. DSWD Field Office 1	San Fernando City, LaUnion
2. DSWD Field Office 2	Carig Sur, Tuguegarao
3. DSWD Field Office 3	San Fernando City, Pampanga
4. DSWD Field Office 4A	Muntinlupa City
5. DSWD Field Office 4B	Malate, Manila
6. DSWD Field Office 5	Legaspi City, Albay
7. DSWD Field Office 6	Molo, Iloilo
8. DSWD Field Office 7	Cebu
9. DSWD Field Office 8	Tacloban City, Leyte
10. DSWD Field Office 9	Zamboanga Del Sur

11. DSWD Field Office 10	Misamis Oriental, CDO
12. DSWD Field Office 11	Davao del Sur
13. DSWD Field Office 12	Koronadal City, South Cotabato
14. DSWD Field Office CARAGA	Butuan City, Agusan del Norte
15. DSWD Field Office CAR	Baguio City, Benguet
16. DSWD Field Office NCR	Legarda, Manila

B. Service Coverage

1. Response On-site (24x7, 4 Hours Onsite)

On-site response time is 24x7x4 for all DSWD sites within Metro Manila. All FO's outside metro manila will be on the next available flight. Secure remote access can also be initiated to check and may address all related firewall concerns.

1.1. Resolution Time

The resolution time varies depending on the complexity of the problem reported.

	Business Critical (Fatal - High)	Business Critical (Medium - Impaired)	Non-Business Critical (Low - information)
Number of Hours	0 - 4 hours	0 – 8 hours	1-3 days

1.2. Definition of Terms

1.2.1. Fatal High - Service is down, total system inoperability.

1.2.2. Medium Impaired - Partial System inoperability.

1.2.3. Low Information - Minor system update, patches, business services are up.

1.3. Escalation (24x7)

1.3.1. For technical support or assistance required, the service provider should put in the contact number numbers and other contact information.

Level	Hour Lapsed	Contact Person	Contact Number	Position
I	Initial call within 30 mins			
II	> 4 hours			
III	> 8 hours			

2. Hardware/ Software Support

Since this is a managed service project, all the hardware and accessories are part of the service provider's property. A spare should be provided for the unit as quick replacement in the event of hardware fault.

A transition support should likewise be provided for **at least three (3) months right after the contract ends** (without additional cost on the part of the DSWD) to prevent prolonged service interruption on the part of the Department while the successor service is being implemented.

3. Scope of Responsibility

The scope of work covers the following:

3.1. Supply and delivery of Next Generation Firewall devices.

3.2. Supply and delivery of Next Generation IPS devices.

3.3. Administration and management of firewalls in the perimeter gateway on all 18 sites.

3.4. Maintain, configure, troubleshoot and address all security concerns in the perimeter gateway. **3.5.** Setup and configuration of DSWD security policy. **3.6.** Proactive monitoring of any security breach on the perimeter and update / resolve security issues. **3.7.** Analysis and presentation of log reports and security events. **4. Capacity Building and Technology Transfer** 4.1. Provide specialized training on Next Generation Perimeter Devices for at least two (2) Central Administrators. 4.2. Provide specialized Training/ Certification on Intrusion Prevention/ Basic Hacking Countermeasures for at least 25 personnel from Central and Field Offices. **5. Network Diagram:** Please see **ANNEX "C".** **IV. Project Requirement** **1.** The service provider/ supplier must deploy and configure all devices and updates on an optimal setting, based on industry's best practices. **2.** The service provider must be in the business for at least 10 years. **3.** The service provider must have at least 5 years' experience and expertise in providing professional services such as managed service, maintenance support, on-call troubleshooting, consulting, training and migration services. **4.** The solution offered must have been in the market for at least 5 years. **5.** The service provider must have previously deployed successfully at least once each in Luzon, Visayas, Mindanao and the NCR.	

6. The service provider must allow a transition period of at least 3 months beyond the last contract month to prevent service interruption while successor project is being implemented.	
ANNEX "A" **1. ADDITIONAL SPECIFICATIONS FOR NEXT GENERATION FIREWALLS** **A. Functional Requirements** 1. **Operational Mode** 1.1. The proposed firewalls shall support policy based Network Address Translation (NAT) and Port Address Translation (PAT) and be able to operate in routing/NAT mode. 1.2. The proposed firewalls shall support Denial of Service (DoS) and fragmented packet Transmission Control Protocol (TCP) reassembly, brute force attack, "SYN cookie", "IP spoofing" and malformed packet protection. 1.3. The proposed firewalls shall support transparent and tap mode within the appliance. 1.4. The proposed firewalls shall support 802.1Q Virtual Local Area Networks (VLANs) tagging (in tap, transparent, layer 2 and layer 3). 1.5. The proposed firewalls shall support dual IPv4 and IPv6 stacks application control and threat inspection support in tap mode, transparent mode, layer 2 and layer 3. 1.6. The proposed firewalls shall support logical Ethernet sub-interfaces tagged and untagged. 1.7. The proposed firewalls shall support the ability to circumvent the route lookup process and the subsequent Policy-Based Forwarding (PBF)	

lookup for return traffic (server to client). The firewalls shall use the original incoming interface as the egress interface. However, if the source IP is in the same subnet as the incoming interface on the firewalls, symmetric return shall not take effect. 1.8. The proposed firewalls shall support policy based forwarding based on zone, source or destination address, source or destination port, application and Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial In User Service (RADIUS) user or user groups. 1.9. The proposed firewalls shall support policy based forwarding based on zone, source or destination address, source or destination port, application and Active Directory (AD)/ Lightweight Directory Access Protocol (LDAP) Remote Authentication Dial In User Service (RADIUS) user or user groups. 1.10. The proposed firewalls shall support IPv6 routing for virtual routers. 2. **Firewalls Management** 2.1. The proposed firewalls solution shall be managed from Web-based Graphical User Interface (GUI) and Command-Line Interface (CLI). 2.2. The proposed firewalls shall be able to manage itself without the need for external servers or appliances, at the same time with an option to be managed centrally. 2.3. The proposed firewalls shall have a dedicated management port that has separate routing tables from the other production interfaces. 2.4. The proposed firewalls management shall be able to granularly assign management functions for each	

management user group or for individual user. 2.5. The proposed firewalls are able to schedule log exports using SCP or FTP protocol. 2.6. The proposed firewalls shall have a reporting management system capable of generating reports on a manual ad-hoc or schedule (daily, weekly, monthly, etc.) basis. 2.7. The proposed firewalls shall be able to generate reports on individual user ID with (but not limited to) the following activities, Application Usage, accessed websites & URL Categories. 3. **Policy Based Controls** The proposed firewall shall support: 3.1. policy control by port and/ or protocol; 3.2. policy control based on application or application category; 3.3. policy control based on user or user group; 3.4. policy control based on IP address; 3.5. policy control by country code; 3.6. per policy Secure Shell (SSH) decryption and inspection; 3.7. IPv6 rules/ objects; and, 3.8. multicast rules/ objects. 4. **Application Security Policy** 4.1. The proposed firewalls shall support network traffic classification, which identifies applications across all ports irrespective of port/protocol/evasive tactics. 4.2. The proposed firewalls shall have multiple mechanisms for classifying	

applications and application identification technology based upon Intrusion Prevention System (IPS) or deep packet inspection. 4.3. The proposed firewalls shall provide the ability to allow the organization to write its own customized application identification signature for new applications not in the current application database or for any in-house applications. 4.4. The proposed firewalls shall include a searchable list of currently identified applications with explanation and links to external sites for further clarification. 4.5. The proposed firewalls shall allow dynamic updates of the application database (DB) and not require a service restart or reboot. 4.6. The proposed firewalls shall warn the end-user with a customizable page when the application is blocked. 4.7. The proposed firewalls shall support user-identification allowing AD, LDAP, RADIUS groups, or users to access a particular application, while denying others. 5. **URL Filtering** 5.1. The proposed firewalls shall support URL filtering/ categorization and have databases stored locally on the appliance. 5.2. The proposed firewalls shall support logs populated with end user activity reports for site monitoring within the local firewalls. 5.3. The proposed firewalls shall support URL filtering policies by AD/ LDAP user, user group, machines and IP address/ range.	

6. **Threat Prevention** 6.1. The proposed firewalls shall support IPS features on the proposed firewalls appliance and antivirus and anti-spyware. 6.2. The proposed firewalls shall perform stream based antivirus and anti-spyware and not store-and-forward traffic inspection. 6.3. The proposed firewalls shall block known network and application-layer vulnerability exploits. 7. **Data Filtering** 7.1. The proposed firewalls shall support file identification by signature and not file extensions. 7.2. The proposed firewalls shall unpack zipped file for packet inspection. 8. **User Identification** 8.1. The proposed firewalls shall support authentication services for AD, LDAP, eDirectory, RADIUS, Kerberos and client certificate. 8.2. The proposed firewalls shall support the creation of a security policy based on AD Users and Groups in addition to source/ destination IP. 8.3. The proposed firewalls shall support user identification in policy without installing an agent on individual endpoints. 8.4. The proposed firewalls shall populate and correlate all logs with user identity (traffic, IPS, URL, data, etc) without any additional products or modules in real-time. 9. **SSL/ SSH Decryption** 9.1. The proposed firewalls shall be able to identify, decrypt and evaluate	

SSL/SSH traffic in an outbound and inbound connection. 9.2. The proposed firewalls shall be able to block SSL sessions with expired server certs. 9.3. The proposed firewalls shall be able to block SSL sessions with untrusted server certs. 9.4. The proposed firewalls shall be able to restrict certificate extensions to limit the purposes for which the generated certificate will be used. 9.5. The proposed firewalls shall be able to block SSL and SSH sessions for unsupported modes (version, cipher suites). 9.6. The proposed firewalls shall be able to decrypt in tap, transparent, layer 2 and layer 3 modes. 10. **Modern Malware Prevention** 10.1 The proposed firewalls are able to provide detection for unknown Malware by using sandboxing technology. Furthermore, it is able to support automatic creation of signatures to detect the unknown malware within 24-hours after detection. 10.2 The proposed firewall is able to provide an on-box reporting of the unknown Malware i.e. replication behavior, command-and-control server info, file downloading, etc. 10.3 When an unknown malware is detected, the proposed firewalls are able to provide the option of prompting the user (via a customized web page) as well as allowing the user to decide whether to upload or download the suspected malicious content.	

10.4 The proposed firewalls shall support in-line control of malware infection and command/control traffic. 10.5 The proposed firewalls shall support DNS-based signatures to detect specific DNS lookups for hostnames that have been associated with malware. 11. **Client Remote Access** 11.1. The proposed firewalls shall allow remote users to access the internal corporate network by automatically establishing either an SSL or IPSec-based VPN connection depending on location and configuration. 11.2. The proposed firewalls shall provide Remote Access agent that supports various Client Platforms i.e. Mac OSX, Windows 7, etc. 11.3. The proposed firewalls remote access agent shall be provided a host information profile (i.e. patch level of OS, status of Anti-Virus software or Host-based IPS, etc.) to the firewalls to ascertain whether the host meets the required security requirement before allowing access into the internal corporate network. 11.4. The proposed firewalls remote access agent shall be able to determine whether the client is within the internal corporate network. If its not, it shall be able to automatically connect to the firewalls and establish a secure tunnel (via SSL or IPSec VPN). 11.5. The proposed firewalls shall be able to authenticate remote users via AD, LDAP, eDirectory, RADIUS, Kerberos and client certificate. 12. **Internet Protocol Version 6 (IPv6) Requirements** 12.1 The Tenderer shall furnish/design the firewalls appliance (also known as	

'Infrastructure' to support the co-existence of IPv4 and IPv6. If it is not compliant, the Tenderer shall advise the roadmap and propose how the system can be upgraded. 13. **Connectivity** 13.1. The propose the Next Generation Firewalls Appliance that will support operations in the following scenarios, but not limited to: 13.1.1. Connect to legacy network and application, which supports IPv4 only. 13.1.2. Connect to local Internet Service Provider (ISP) and IPv6 service and the end-user using IPv6 only. 13.1.3. Connect to local ISP and IPv4 service and the remote ISP and IPv6 service, and the remote end-user using IPv6 only. 13.2. The proposed firewalls shall support the following IPv6 features, but not limited to: 13.2.1. Able to support Network Address Translation from IPv6 to IPv4. 13.2.2. Able to support Stateless Address Auto-Configuration (SLAAC) for IPv6-configured interfaces. The proposed firewalls shall be able to send router advertisement (RA) messages on connected links in order to inform hosts of the IPv6 prefixes that they can use for address configuration. 13.2.3. Able to support routing of IPv6 traffic over an IPSec tunnel established between IPv4 endpoints. 13.2.4. Able to provide IPv6 connectivity for firewalls administrative controls (i.e. Syslog, SNMP, DNS, NTP,	

Admin Authentication Sources, etc.). 14. **Maintenance and Support** 14.1. The Tenderer shall provide information on whether any patches, upgrades or additional hardware and/or software and/or services are needed to be purchased or installed in order for the proposed hardware and software to support the co-existence of IPv4 and IPv6 environment. **2. ADDITIONAL SPECIFICATIONS FOR A CENTRALIZED FIREWALL MANAGEMENT SYSTEM** 2.1. Central Visibility and Global Policy Control 2.1.1. Graphical view of applications, URL, threat and data traversing all firewalls 2.1.1.1. Capable of displaying summary of applications running on the network, the users and the security impact. 2.1.1.2. Nationwide Admin will have the capabilities to manage all Next Gen Firewalls deployed at any remote site of DSWD. Same access with the local admin. 2.1.1.3. Nationwide admin can create and enforce policies/templates on any individual devices or all devices. 2.1.2. Can control application enablement, QoS, URL filtering and other policies across nationwide network of DSWD 2.2. Traffic Monitoring and reporting for Analysis and Forensic 2.2.1. Traffic monitoring and reporting tools available both local and National (whole DSWD nationwide network).	

2.2.2. Access to all Logs (log viewer), either local, individual or all devices. 2.2.3. Custom Reporting: both predefined and customized / grouped reports can be done. 2.2.4. User activity Reports: aggregate and individual device/users can be created. 2.2.5. Log forwarding: aggregated reports from all devices in the nationwide network of DSWD can be created. 2.3. Number of Devices Supported for centralized Management. It must support all remote sites of DSWD with the Next Generation firewall: **At least 25 devices.** 2.4. High Availability Support: must be capable of Active/Passive modes. 2.5. Admin Authentication: must be capable of Local and Radius databases. 2.6. Management Tools and APIs: GUI, Command Line and XML-based REST API. 2.7. Storage: at least 16TB with RAID storage. 2.8. Rack Mount: can be deployed on a rack.	
ANNEX "B" **1. ADDITIONAL FEATURE SPECIFICATIONS FOR NEXT GENERATION INTRUSION PREVENTION SYSTEMS (IPS) FOR DSWD** **1.1. Advanced Threat Protection** 1.1.1. The proposed solution must have at least TEN (10) gigabits per second throughput while having application visibility control and intrusion prevention active. 1.1.2. The proposed solution platforms must be based on a hardened operating system.	

1.1.3. The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes. 1.1.4. The detection engine should support Layer 2 deployment so that it provides packet switching and inspection between two or more network segments. 1.1.5. The detection engine should support Layer 3 deployment where it can route and inspect traffic between two or more interfaces. 1.1.6. Detection rules must be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules. 1.1.7. Detection rules provided by the vendor must be documented, with full descriptions of the identity, nature, and severity of the associated vulnerabilities and threats being protected against. 1.1.8. The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.). 1.1.9. The detection engine must be capable of detecting variants of known threats, as well as new threats (i.e., so-called "unknown threats"). 1.1.10. The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.	

1.1.11.	The detection engine must inspect not only Network Layer details and information resident in packet headers, but a broad range of protocols across all layers of the computing stack and packet payloads as well.	
1.1.12.	The detection engine must be resistant to various URL obfuscation techniques common to HTML-based attacks.	
1.1.13.	The solution must incorporate measures to minimize the occurrence of both false positives and false negatives (i.e., mistaken and missed detection events, respectively).	
1.1.14.	The solution must be capable of detecting multi-part or extended threats by aggregating and correlating the multiple, disparate events associated with them.	
1.1.15.	The detection engine must be capable of inspecting traffic associated with different network segments differently (as opposed to having only one policy per interface).	
1.1.16.	Sensors must be capable of performing packet-level forensics and capturing raw packet data in response to individual events without significant performance degradation.	
1.1.17.	The detection engine must support multiple options for directly responding to events, such as monitor only, block offending traffic, replace packet payload, and capture packets.	
1.1.18.	The management platform must be capable of setting thresholds such that multiple instances of specific events are required before an alert is issued.	
1.1.19.	The solution must be capable of detecting and blocking IPv6 attacks.	
1.1.20.	The solution must provide IP reputation feed that comprised of	

several regularly updated collections of IP addresses determined by the proposed security vendor to have a poor reputation. 1.1.21. The solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist. 1.1.22. The solution must have the option of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network (SHA-256 and target IP address should be given to aid remediation efforts). 1.1.23. The solution must have a network file trajectory feature that can provide a visual, interactive representation of the path an infected file takes across the network, to help us understand the broader impact, context, and spread of malware across the network and endpoints. This view depicts point of entry, propagation, protocols used, and the users or endpoints involved in the transfer. 1.1.24. The solution must support geolocation lookup. **1.2. Real-Time Contextual Awareness** 1.2.1. The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance. 1.2.2. The solution must be capable of passively gathering information about session flows for all monitored hosts,	

	including start/end time, ports, services, and amount of data.	
1.2.3.	The solution must be capable of passively detecting pre-defined services, such as FTP, HTTP, POP3, Telnet, etc., as well as custom services.	
1.2.4.	The solution must be capable of storing user-defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.	
1.2.5.	The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.	
1.2.6.	The solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.	
1.2.7.	The solution must be capable of identifying "Jailbroken" mobile devices, which can help to enforce mobile device usage policies on the network.	
1.2.8.	The solution must provide a detailed, interactive graphical summary that includes data on applications, application statistics, connections, intrusions events, hosts, servers, users, file-types, malwares and relevant URLs. These data should be presented in the form of vivid line, bar, pie and donut graphs accompanied by detailed lists (Administrator should easily create and apply custom filters to fine-tune the analysis).	
1.2.9.	The aforementioned network and user intelligence must be passively gathered	

using existing IPS devices (no separate hardware required). **1.3. Intelligent Security Automation** 1.3.1. The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events. 1.3.2. The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward. 1.3.3. The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention. 1.3.4. The solution must be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports. 1.3.5. The solution must be capable of defending against IPS-evasion attacks by automatically using the most appropriate defragmentation and stream reassembly routines for all traffic based on the characteristics of each destination host. **1.4. Control Compliance** 1.4.1. The solution must have the option for integrating application control to reduce risks associated with applications usage and client-side attacks. It should provide a means of	

	enforcing acceptable use policies of up to 2000 application detectors.	
1.4.2.	The solution must support creation of user-defined application protocol detectors.	
1.4.3.	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions: - Protocols: HTTP, SMTP, IMAP, POP; - Direction: Upload, Download, Both; and, - File Types: Office Documents, Archive, Multimedia, Executable, PDF, Encoded, Graphics, and System Files.	
1.4.4.	The proposed solution should provide an option to include URL filtering for enforcing Internet content filtering so as to reduce web born threats and improve productivity. Each URL in the data set must has an associated category and reputation. URL category is a general classification for the URL while URL reputation represents how likely the URL is to be used for purposes that might be against the organization's security policy.	
1.4.5.	The solution must provide capabilities for establishing and enforcing host compliance policies and alerting on violations.	
1.4.6.	The solution must be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.	
1.4.7.	The solution must be capable of easily identifying all hosts that exhibit a	

specific attribute or non-compliance condition. **1.5. Network Behavior Analysis (NBA)** 1.5.1. The solution must provide a full-featured NBA capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter IPS). This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines. 1.5.2. The NBA capability must provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and performance degradations. 1.5.3. The NBA capability must provide the ability to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events. 1.5.4. The NBA capability must provide the option of supplying endpoint intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization. 1.5.5. The same network devices used for IPS must also be used as part of the NBA capability. No NBA-only device should be required. 1.5.6. The same management platform used for IPS must also be used to manage the NBA capability. No NBA-only management components should be required. **1.6. Management and Usability** 1.6.1. The management platform must be capable of centralized, life cycle management for all sensors.	

1.6.2. The management platform must be delivered in virtual appliance form factor (management system and UI must provide the same features and functions as in the physical appliance). 1.6.3. The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events. 1.6.4. The management platform must be accessible via a web-based interface and ideally with no need for additional client software. 1.6.5. The management platform must provide a highly customizable dashboard. 1.6.6. The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows. 1.6.7. The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication. 1.6.8. The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application. 1.6.9. The management platform must include one or more default (i.e., pre-defined) detection policy configurations to help simplify initial deployment. 1.6.10. The management platform must be capable of grouping both sensors and policies to help simplify configuration management.	

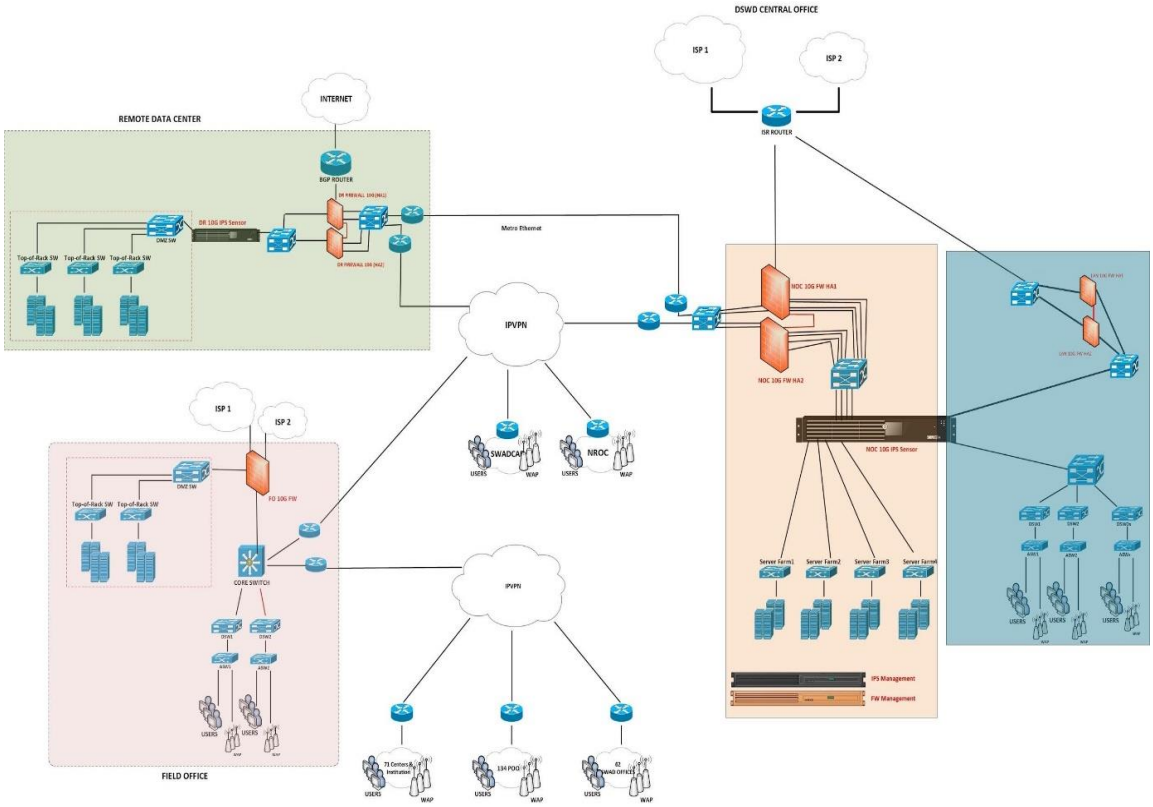
1.6.11. The management platform must provide the capability to easily view, enable, disable, and modify individual rules, as well as groups or categories of rules. 1.6.12. The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors. 1.6.13. The management platform must be capable of backup and rollback for sensor configurations and the management platform itself. 1.6.14. The management platform must include flexible workflow capabilities for managing the complete life cycle of an event, from initial notification through to any response and resolution activities that might be required. 1.6.15. The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered. 1.6.16. The management platform must support both internal and external databases/systems for storage of event data, logs, and other system-generated information. 1.6.17. The management platform must be capable of synchronizing time between all components of the system via NTP. 1.6.18. The management platform must be capable of logging all administrator activities, both locally and to a remote log server. **1.7. Reporting and Alerting** 1.7.1. The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete	

customization and generation of new reports. 1.7.2. The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries. 1.7.3. The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV. 1.7.4. The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG). **1.8. Reliability and Availability** 1.8.1. Sensors must support built-in capability of failing open, such that communications traffic is still allowed to pass if the inline sensor goes down. 1.8.2. The product must support "Lights Out Management" capability where remote upgrade, restore, and downgrade functionality without physical access to the appliance being required. 1.8.3. The sensor platforms must support a range of models, including modular design on the high-end and standard connectivity options on the low-end. The high-end sensor platforms must be capable of offering additional flexibility through stacking to increase throughput as your inspection needs grow without using external load balancing solutions. 1.8.4. The management platform must be capable of monitoring the health of all components and issuing alerts for anomalous conditions. 1.8.5. Intra-system communications must be secure.	

1.8.6. The supplier must have a detailed process for customer submission of product-related faults and the resolution of those faults, including provisions for escalation of critical or unresolved issues. **1.9. Third-Party Integration** 1.9.1. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable automatic response to threats by external components and remediation applications, such as routers, firewalls, patch management systems, etc. 1.9.2. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools. 1.9.3. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to receive information from external sources, such as configuration management databases, vulnerability management tools, and patch management systems, for threat correlation and IT policy compliance purposes. 1.9.4. The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to network management systems.	

ANNEX "C"

NETWORK DIAGRAM



Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

Section VIII. Checklist of Technical and Financial Documents

Checklist of Technical and Financial Documents

I. TECHNICAL COMPONENT ENVELOPE

Class "A" Documents

Legal Documents

☐ (a) Valid PhilGEPS Registration Certificate (Platinum Membership) (all pages);
or

☐ (b) Registration certificate from Securities and Exchange Commission (SEC), Department of Trade and Industry (DTI) for sole proprietorship, or Cooperative Development Authority (CDA) for cooperatives or its equivalent document,
and

☐ (c) Mayor's or Business permit issued by the city or municipality where the principal place of business of the prospective bidder is located, or the equivalent document for Exclusive Economic Zones or Areas;
and

☐ (d) Tax clearance per E.O. No. 398, s. 2005, as finally reviewed and approved by the Bureau of Internal Revenue (BIR).

Technical Documents

☐ (e) Statement of the prospective bidder of all its ongoing government and private contracts, including contracts awarded but not yet started, if any, whether similar or not similar in nature and complexity to the contract to be bid; **and**

☐ (f) Statement of the bidder's Single Largest Completed Contract (SLCC) similar to the contract to be bid, except under conditions provided for in Sections 23.4.1.3 and 23.4.2.4 of the 2016 revised IRR of RA No. 9184, within the relevant period as provided in the Bidding Documents; **and**

☐ (g) Original copy of Bid Security. If in the form of a Surety Bond, submit also a certification issued by the Insurance Commission;
or
Original copy of Notarized Bid Securing Declaration; **and**

☐ (h) Conformity with the Technical Specifications, which may include production/delivery schedule, manpower requirements, and/or after-sales/parts, if applicable; **and**

☐ (i) Original duly signed Omnibus Sworn Statement (OSS);
and Original Notarized Secretary's Certificate in case of a corporation, partnership, or cooperative; or Original Special Power of Attorney in case of a single proprietorship; or Original Special Power of Attorney of all members of the joint venture giving full power and authority to its officer to sign the OSS and do acts to represent the Bidder.

Financial Documents

☐ (j) The Supplier's audited financial statements, showing, among others, the Supplier's total and current assets and liabilities, stamped "received" by the BIR or its duly accredited and authorized institutions, for the preceding calendar year which should not be earlier than two (2) years from the date of bid submission; **and**

☐ (k) The prospective bidder's computation of Net Financial Contracting Capacity (NFCC);

or

A committed Line of Credit from a Universal or Commercial Bank in lieu of its NFCC computation.

Class "B" Documents

☐ (l) If applicable, a duly signed joint venture agreement (JVA) in case the joint venture is already in existence;

or

duly notarized statements from all the potential joint venture partners stating that they will enter into and abide by the provisions of the JVA in the instance that the bid is successful.

II. FINANCIAL COMPONENT ENVELOPE

☐ (m) Original of duly signed and accomplished Financial Bid Form; **and**

☐ (n) Original of duly signed and accomplished Price Proposal Form; **and**

☐ (o) Original of duly signed and accomplished Price Schedule(s).

Other documentary requirements under RA No. 9184 (as applicable)

☐ (p) *[For foreign bidders claiming by reason of their country's extension of reciprocal rights to Filipinos]* Certification from the relevant government office of their country stating that Filipinos are allowed to participate in government procurement activities for the same item or product.

☐ (q) Certification from the DTI if the Bidder claims preference as a Domestic Bidder or Domestic Entity.

Section IX. Bidding Forms

TABLE OF CONTENTS

Bid Form

Date: _____

Invitation to Bid No.: GOP/20-DSWD-060

To: [name and address of Procuring Entity]

Having examined the Philippine Bidding Documents (PBDs) including the Supplemental or Bid Bulletin Numbers *[insert numbers]*, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to *[supply/deliver/perform] [description of the Goods]* in conformity with the said PBDs for the sum of *[total Bid amount in words and figures]* or the total calculated bid price, as evaluated and corrected for computational errors, and other bid modifications in accordance with the Price Schedules attached herewith and made part of this Bid. The total bid price includes the cost of all taxes, such as, but not limited to: *[specify the applicable taxes, e.g. (i) value added tax (VAT), (ii) income tax, (iii) local taxes, and (iv) other fiscal levies and duties]*, which are itemized herein or in the Price Schedules,

If our Bid is accepted, we undertake:

(a) to deliver the goods in accordance with the delivery schedule specified in the Schedule of Requirements of the Philippine Bidding Documents (PBDs);

(b) to provide a performance security in the form, amounts, and within the times prescribed in the PBDs;

(c) to abide by the Bid Validity Period specified in the PBDs and it shall remain binding upon us at any time before the expiration of that period.

Until a formal Contract is prepared and executed, this Bid, 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 Calculated Bid or any Bid you may receive.

We certify/confirm that we comply with the eligibility requirements pursuant to the PBDs.

The undersigned is authorized to submit the bid on behalf of *[name of the bidder]* as evidenced by the attached *[state the written authority]*.

We acknowledge that failure to sign each and every page of this Bid Form, including the attached Schedule of Prices, shall be a ground for the rejection of our bid.

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

Price Schedule for Goods Offered from Abroad

Name of Bidder: _____ Invitation to Bid No. _____

Page ____ of ____

1	2	3	4	5	6	7	8	9
Item	Description	Country of origin	Quantity	Unit price CIF port of entry (specify port) or CIP named place (specify border point or place of destination)	Total CIF or CIP price per item (col. 4 x 5)	Unit Price Delivered Duty Unpaid (DDU)	Unit price Delivered Duty Paid (DDP)	Total Price delivered DDP (col 4 x 8)

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Price Schedule for Goods Offered from Within the Philippines

Name of Bidder: _____ Invitation to Bid No. _____
Page ____ of ____

1	2	3	4	5	6	7	8	9	10
Item	Description	Country of origin	Quantity	Unit price EXW per item	Transportation and Insurance and all other costs incidental to delivery, per item	Sales and other taxes payable if Contract is awarded, per item	Cost of Incidental Services, if applicable, per item	Total Price, per unit (col 5+6+7+8)	Total Price delivered Final Destination (col 9) x (col 4)

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Price Proposal Form

Date: _____

Invitation to Bid No.: GOP/20-DSWD-060

Subscription to Managed Services for DSWD Complete Suite of Primary ICT Security Devices

Particulars	Quantity	Unit Price *(in PHP)*	Total Price *(in PHP)*
NextGen Firewall (SLA/License)			
DSWD Central Office LAN (NGFW) (HA Mode)	2 units		
DSWD Central Office WAN (NGFW 10G) (HA Mode)	2 units		
Central Office (NGFW Mgmt)	1 unit		
Remote Data Center (NGFW 10G) (HA Mode)	2 units		
DSWD Field Offices (10G NGFW incl. spare)	17 units		
NextGen IPS Licenses (SLA/Licenses)			
DSWD Central Office (IPS Mgmt)	1 unit		
DSWD Central Office (IPS Sensor 10G)	1 unit		
Remote Data Center (IPS Sensor 10G)	1 unit		
Trainings (set of participants)	2 units		
Annual Support and Maintenance	1 unit		
		TOTAL CONTRACT PRICE	

NOTE: In case of discrepancy between unit price and total price, the unit price will prevail. Total Contract Price is inclusive of all applicable taxes.

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

BID SECURING DECLARATION FORM

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

BID SECURING DECLARATION
Invitation to Bid No.: *[Insert Reference number]*

To: *[Insert name and address of the Procuring Entity]*

I/We, the undersigned, declare that:

1. I/We understand that, according to your conditions, bids must be supported by a Bid Security, which may be in the form of a Bid-Securing Declaration.

2. I/We accept that: (a) I/we will be automatically disqualified from bidding for any procurement contract with any procuring entity for a period of two (2) years upon receipt of your Blacklisting Order; and, (b) I/we will pay the applicable fine provided under Section 6 of the Guidelines on the Use of Bid Securing Declaration, within fifteen (15) days from receipt of the written demand by the procuring entity for the commission of acts resulting to the enforcement of the bid securing declaration under Sections 23.1(b), 34.2, 40.1 and 69.1, except 69.1(f),of the IRR of RA No. 9184; without prejudice to other legal action the government may undertake.

3. I/We understand that this Bid Securing Declaration shall cease to be valid on the following circumstances:

   (a) Upon expiration of the bid validity period, or any extension thereof pursuant to your request;

   (b) I am/we are declared ineligible or post-disqualified upon receipt of your notice to such effect, and (i) I/we failed to timely file a request for reconsideration or (ii) I/we filed a waiver to avail of said right; and

   (c) I am/we are declared the bidder with the Lowest Calculated Responsive Bid, and I/we have furnished the performance security and signed the Contract.

IN WITNESS WHEREOF, I/We have hereunto set my/our hand/s this ____ day of *[month] [year]* at *[place of execution]*.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]
[Format shall be based on the latest Rules on Notarial Practice]

Contract Agreement Form

CONTRACT AGREEMENT

THIS AGREEMENT made the _____ day of _____ 20_____ between **DEPARTMENT OF SOCIAL WELFARE AND DEVELOPMENT** of the Philippines (hereinafter called "the Entity") of the one part and *[name of Supplier]* of *[city and country of Supplier]* (hereinafter called "the Supplier") of the other part;

WHEREAS, the Entity invited Bids for certain goods and ancillary services, particularly *[brief description of goods and services]* and has accepted a Bid by the Supplier for the supply of those goods and services in the sum of *[contract price in words and figures in specified currency]* (hereinafter called "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

1. In this Agreement words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents as required by the 2016 revised Implementing Rules and Regulations of Republic Act No. 9184 shall be deemed to form and be read and construed as integral part of this Agreement, *viz.*:

   i. Philippine Bidding Documents (PBDs);
      i. Schedule of Requirements;
      ii. Technical Specifications;
      iii. General and Special Conditions of Contract; and
      iv. Supplemental or Bid Bulletins, if any

   ii. Winning bidder's bid, including the Eligibility requirements, Technical and Financial Proposals, and all other documents or statements submitted;

      Bid form, including all the documents/statements contained in the Bidder's bidding envelopes, as annexes, and all other documents submitted (*e.g.*, Bidder's response to request for clarifications on the bid), including corrections to the bid, if any, resulting from the Procuring Entity's bid evaluation;

   iii. Performance Security;

   iv. Notice of Award of Contract; and the Bidder's conforme thereto; and

   v. Other contract documents that may be required by existing laws and/or the Procuring Entity concerned in the PBDs. **Winning bidder agrees that additional contract documents or information prescribed by the GPPB that are subsequently required for submission after the contract execution, such as the Notice to Proceed, Variation Orders, and Warranty Security, shall likewise form part of the Contract.**

3. In consideration for the sum of *[total contract price in words and figures]* or such other sums as may be ascertained, *[Named of the bidder]* agrees to *[state the object of the contract]* in accordance with his/her/its Bid.

4. The *[Name of the procuring entity]* agrees to pay the above-mentioned sum in accordance with the terms of the Bidding.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of the Republic of the Philippines on the day and year first above written.

_____	_____
[Insert Name and Signature]	*[Insert Name and Signature]*
_____	_____
[Insert Signatory's Legal Capacity]	*[Insert Signatory's Legal Capacity]*
for:	for:
_____	_____
[Insert Procuring Entity]	*[Insert Name of Supplier]*

Acknowledgment

[Format shall be based on the latest Rules on Notarial Practice]

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 or authorized representative 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, or authorized representative of *[Name of Bidder]*, I have full power and authority to do, execute and perform any and all acts necessary to participate, submit the bid, and to sign and execute the ensuing contract for *[Name of the Project]* of the *[Name of the Procuring Entity], as shown in the attached duly notarized Special Power of Attorney*;

   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 to participate, submit the bid, and to sign and execute the ensuing contract for *[Name of the Project]* of the *[Name of the Procuring Entity]*, as shown in the attached *[state title of attached document showing proof of authorization (e.g., duly notarized Secretary's Certificate, Board/Partnership Resolution, or Special Power of Attorney, whichever is applicable;)]*;

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, **by itself or by relation, membership, association, affiliation, or controlling interest with another blacklisted person or entity as defined and provided for in the Uniform Guidelines on Blacklisting;**

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: The owner or sole proprietor is 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; and

8. *[Name of Bidder]* is aware of and has undertaken the responsibilities as a Bidder in compliance with the Philippine Bidding Documents, which includes:

   (a) Carefully examining all of the Bidding Documents;

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

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

   (d) Inquiring or securing 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.

10. **In case advance payment was made or given, failure to perform or deliver any of the obligations and undertakings in the contract shall be sufficient grounds to constitute criminal liability for Swindling (Estafa) or the commission of fraud with unfaithfulness or abuse of confidence through misappropriating or converting any payment received by a person or entity under an obligation involving the duty to deliver certain goods or services, to the prejudice of the public and the government**

of the Philippines pursuant to Article 315 of Act No. 3815 s. 1930, as amended, or the Revised Penal Code.

IN WITNESS WHEREOF, I have hereunto set my hand this __ day of ___, 20__ at _____, Philippines.

[Insert NAME OF BIDDER OR ITS AUTHORIZED REPRESENTATIVE]
[Insert signatory's legal capacity]
Affiant

[Jurat]

[Format shall be based on the latest Rules on Notarial Practice]

Bank Guarantee Form for Advance Payment

To: *[name and address of PROCURING ENTITY]*
[name of Contract]

Gentlemen and/or Ladies:

In accordance with the payment provision included in the Special Conditions of Contract, which amends Clause **Error! Reference source not found.** of the General Conditions of Contract to provide for advance payment, *[name and address of Supplier]* (hereinafter called the "Supplier") shall deposit with the PROCURING ENTITY a bank guarantee to guarantee its proper and faithful performance under the said Clause of the Contract in an amount of *[amount of guarantee in figures and words]*.

We, the *[bank or financial institution]*, as instructed by the Supplier, agree unconditionally and irrevocably to guarantee as primary obligator and not as surety merely, the payment to the PROCURING ENTITY on its first demand without whatsoever right of objection on our part and without its first claim to the Supplier, in the amount not exceeding *[amount of guarantee in figures and words]*.

We further agree that no change or addition to or other modification of the terms of the Contract to be performed thereunder or of any of the Contract documents which may be made between the PROCURING ENTITY and the Supplier, shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition, or modification.

This guarantee shall remain valid and in full effect from the date of the advance payment received by the Supplier under the Contract until *[date]*.

Yours truly,

Signature and seal of the Guarantors

_____
[name of bank or financial institution]

_____
[address]

_____
[date]

Certification from Insurance Commission

NOTE: *Use this template for the required "Certification from the Insurance Commission", which shall accompany surety bonds issued for purposes of Bid Security and Performance Security.*

[Insurance Commission Letterhead]

CERTIFICATION

This is to certify that *[insert Name of Insurance Company]* is an authorized insurance company and licensed to transact general insurance business in the Philippines for such lines as Fire, Marine, Casualty and Surety under *[insert Certificate of Authority Number]* effective *[insert date of period of effectivity]*, unless sooner revoked or suspended for cause.

It is certified, moreover, that *[insert Name of Insurance Company]* is likewise authorized under Administrative Order No. 30 to underwrite and issue Performance Bonds, Bidder's Bonds, and Surety Bonds, callable on demand in favor of the various agencies and instrumentalities of the government pursuant to the Revised Implementing Rules of RA.9184.

It is further certified that *[insert Name of Insurance Company]* issued a surety bond under *[insert Bond No.]* to *[insert Name of Service Provider or Supplier]* in favor of **Department of Social Welfare and Development** in the amount of *[insert amount]* for the *[insert Name of the Project).*

This certification is issued upon the request of *[insert Name of the Authorized Representative]* of *[insert Name of Insurance Company]*, pursuant to Section 39.2(c) of the Revised Implementing Rules and Regulations of RA9184.

Issued on the *[insert date]* in *[insert Place]*.

For the Insurance Commissioner
[insert name of Authorized Representative]
[insert Position and Office]
Paid under [insert Official Receipt No.]

Statement of All On-Going Government and Private Contracts, Including Contracts Awarded but Not Yet Started, Whether Similar or Not Similar in Nature and Complexity to the Contract to be Bid

Business Name: _____
Business Address: _____

A. Government

Nature of Contract (Project Title)	a. Owner's Name b. Address c. Contact Nos.	Project Cost	Bidder's Role		a. Date Awarded b. Date Started c. Target Date of Completion	% of Accomplishment		Value of Outstanding Works (Undelivered Portion)
			Description	%		Planned	Actual	
1.	a. b. c.				a. b. c.			
2.	a. b. c.				a. b. c.			

B. Private

Nature of Contract (Project Title)	a. Owner's Name b. Address c. Contact Nos.	Project Cost	Bidder's Role		a. Date Awarded b. Date Started c. Target Date of Completion	% of Accomplishment		Value of Outstanding Works (Undelivered Portion)
			Description	%		Planned	Actual	
1.	a. b. c.				a. b. c.			
2.	a. b. c.				a. b. c.			

Note: *The following documents must be available upon request of the Bids and Award Committee (BAC) or designated Technical Working Group (TWG) during Post-Qualification to support this statement: (a)* ***Contract or Purchase Order****, (b)* ***Official Receipt(s) or Sales Invoice*** *or (c)* ***User's Certificate of Acceptance/Completion***

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

Statement of Single Largest Completed Contract (SLCC)[2] Similar to the Contract to be Bid

Business Name: _____
Business Address: _____

Nature of Contract (Project Title)	**a. Owner's Name**	**Project Cost**	**Bidder's Role**		**a. Date Awarded**
	b. Address				**b. Date Started**
	c. Contact Nos.		**Description**	**%**	**c. Date Completed**
	a.				a.
	b.				b.
	c.				c.

Note: *The following documents must be attached to support this statement: (a)* ***Official Receipt(s) or Sales Invoice*** *or (b)* ***User's Certificate of Acceptance/Completion***

Name: _____

Legal Capacity: _____

Signature: _____

Duly authorized to sign the Bid for and behalf of: _____

Date: _____

[2] *The Bidder must have completed, within the period specified in the Invitation to Bid and ITB Clause 5.3(a), a single contract that is similar to the project to be bid, equivalent to a percentage (%) of the ABC specified in ITB Clause 5.3(b).*


Republic of the Philippines
gppb
Government Procurement Policy Board