

# Special Conditions of Contract

| GCC Clause |  |
|------------|--|
| 1.1(g)     | The Procuring Entity is<br><br>BASES CONVERSION AND DEVELOPMENT AUTHORITY  |
| 1.1(i)     | The Supplier is <i>[to be inserted at the time of contract award]</i> .  |
| 1.1(j)     | The Funding Source is<br><br>The Government of the Philippines (GOP) through BCDA's Corporate Operating Budget in the amount not to exceed <b>FIVE MILLION FIVE HUNDRED THOUSAND PESOS (Php 5,500,000.00)</b> , inclusive of all applicable taxes, fees and other charges. |
| 1.1(k)     | The Project Site is at:<br><br>BCDA Corporate Center, 2/F Bonifacio Technology Center, 31 <sup>st</sup> St., Corner 2 <sup>nd</sup> Avenue, Bonifacio Global City, Taguig City   |
| 2.1        | No further instructions.   |
| 5.1        | The Procuring Entity's address for Notices is:<br><br>BCDA Corporate Center, 2nd Floor Bonifacio Technology Center, 31st St., Corner 2nd Avenue, Bonifacio Global City, Taguig City<br><br>The Supplier's address for Notices is: _____                                    |
| 6.2        | The Contract shall be issued in the form of a Purchase Order (PO)<br><br>Delivery of the GOODS shall be made by the Supplier in accordance with the terms specified in Schedule of Requirements.   |
| 10.4       | Not applicable.  |
| 10.5       | Payment using LC is not allowed.   |
| 11.3       | Maintain the GCC Clause.   |
| 13.4(c)    | No further instructions.   |
| 16.1       | None.  |
| 17.3       | <i>Please refer to the Technical Specifications.</i>   |

|      |  |
|------|--|
| 17.4 | Please see Technical Specifications on the details of service during warranty.   |
| 21.1 | <i>If the Supplier is a joint venture, "All partners to the joint venture shall be jointly and severally liable to the Procuring Entity"</i> |

Uncontrolled when printed or emailed



Uncontrolled when printed or emailed

***Section VI. Schedule of Requirements***



## Schedule of Requirements

The delivery schedule expressed as weeks/months stipulates hereafter a delivery date which is the date of delivery to the project site.

| Description                               | Quantity | Delivered, Weeks/Months  |
|---|----------|--|
| Data Center and Network Security Solution | 1        | Within 10 – 60 calendar days from receipt of Purchase Order.<br><br>Project site:<br>BCDA Corporate Center, 2/F<br>Bonifacio Technology Center, 31 <sup>st</sup> St.,<br>Corner 2 <sup>nd</sup> Avenue, Bonifacio Global City, Taguig City |

**Bidder's Authorized Representative:**

\_\_\_\_\_  
Signature over Printed Name

\_\_\_\_\_  
Principal Bidder / Supplier

***Section VII. Technical Specifications  
Compliance Form***

Uncontrolled when printed or emailed



# TECHNICAL SPECIFICATION

| ITEM | SPECIFICATIONS  | Compliance |               |
|------|---|------------|---------------|
| 1    | <b>Data Center and Network Security Solution</b>  | Compliant  | Non-Compliant |
|      | <b>One (1) unit network-wide threat detection and protection appliance</b>  |            |               |
|      | <b><u>General Specifications:</u></b>   |            |               |
|      | Able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections. |            |               |
|      | Support the native Common Event Format (CEF), Log Event Extended Format (LEEF) for Security Information and Event Management (SIEM) log integration.  |            |               |
|      | Anti-APT (Advanced Persistent Threat) solution should perform advanced network detection and analysis of the enterprise's internal network.   |            |               |
|      | Upon detection of the threat, should be able to perform behavior analysis for advance detection   |            |               |
|      | Have event detection capabilities that should include malware type, severity, source and destination of attack.   |            |               |
|      | Provide risk based alerts or logs to help prioritize remediation effort   |            |               |
|      | Deployed on premise along with on premise sandboxing capability   |            |               |
|      | Able to store real payload of the detected threats  |            |               |
|      | Able to store packet captures (PCAP) of all malicious communications detected by sandbox  |            |               |
|      | Use OS sandboxes for detecting zero day malwares. This should not be a CPU or chip based function   |            |               |
|      | Ability to interrupt malicious communication.   |            |               |
|      | No limitation in terms of supported users and limitation should be accounted in terms of only bandwidth.  |            |               |
|      | Support XFF (XForwarded-For) to identify the IP Address of a host in a proxy/Network Address Translation (NAT) environment.   |            |               |
|      | Able to integrate with its own threat intelligence portal for further investigation, understanding and remediation of an attack.  |            |               |
|      | Solution deployment should cause limited interruption to the current network environment.   |            |               |
|      | Should allow BCDA to gain visibility to the internal networks and flag detected threats immediately.  |            |               |
|      | Ability to support out-of-band detection.   |            |               |

*Handwritten signature/initials*

|   |  |  |
|---|--|--|
| Able to detect (lateral moments) movement of the attacker without the need of installing agents on endpoint/server machines   |  |  |
| Should not have any port based limitation and should support all ports.   |  |  |
| Support at least 100+ protocols for inspection.   |  |  |
| Support to monitor traffic from multiple segments like Wide Area Network (WAN), Demilitarized Zone (DMZ), Server Farm, Wi-Fi network, Multiprotocol Label Switching (MPLS) links etc. simultaneously on a single appliance.   |  |  |
| Support up to 5 network segments on a single appliance.   |  |  |
| Able to detect any suspicious communication within and outside of customer's network  |  |  |
| Able to detect communications to known command and control centers  |  |  |
| Able to detect reputation of Uniform Resource Locator (URL) being accessed  |  |  |
| Able to identify and help customer to understand the severity and stage of each attack  |  |  |
| Should have built in capabilities to add exceptions for detections  |  |  |
| Should have capabilities to configure files, IP, URLs and domains to black list or white list   |  |  |
| Should support multiple protocols for inspection. example:- Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), Instant Message (IM), Internet Relay Chat (IRC), Domain Name System (DNS) and P2P protocols, internal direction: Server Message Block (SMB), database protocol (MySQL, MSSQL, Oracle) on a single device |  |  |
| Should have a co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis.  |  |  |
| Must provide a web service interface/Application Programming Interface (API) for customer to customize their own system integration   |  |  |
| Have capabilities to correlate the detections on the device itself.   |  |  |
| Support remote packet capturing to pass the Kerberos traffic from the remote location for analysis  |  |  |
| Should monitor inter-Virtual Machine (VM) traffic on a Port Mirror session.   |  |  |
| Should provide correlated threat data such as: Internet Protocol (IP) addresses, DNS domain names, URLs, filenames, process names, Windows registry entries, file hashes, malware detections and malware families through a portal.   |  |  |


|  |  |  |
|--|--|--|
| Able to run at least 4 parallel sandboxes for analysis of payload.   |  |  |
| Should have option to allow sandbox instances to use a proxy for internet access.  |  |  |
| Support for analysis of embedded URLs in Portable Document Format (PDFs)   |  |  |
| Support IPv6 environments and be able to tap into IPv6 network streams, perform analysis, and output IPv6-based network detection results.   |  |  |
| Should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for advanced threat detection.   |  |  |
| Able to provide detection details including the Common Vulnerabilities and Exposures (CVE)-ID, HTTP referrer and targeted attack campaign name   |  |  |
| Able to provide customizable sandbox to fulfill customer's environments and needs.   |  |  |
| Sandbox must support multiple operating systems and for both 32-bits and 64-bits Operating System (OS)   |  |  |
| Capability to analyze large files. Must be able to support more than 40MB file size  |  |  |
| Sandbox must have the ability to simulate the entire threat behavior. i.e. honeynet and honeypot framework   |  |  |
| Support Windows XP, Windows 7, Windows 8, Windows 10, MS Server 2003 and MS Server 2008 operating environments for sandboxing this requirement should be based on virtual execution and should not be a hardware or chip based function. |  |  |
| The proposed solution should have gray ware detection capabilities.  |  |  |
| The proposed solution should be able to detect any malicious communication within and outside of Customer's network.   |  |  |
| The proposed solution must provide a web service interface/API for Customer to customize their own system integration.   |  |  |
| The Proposed solution should be able to detect Network Attacks and Exploits.   |  |  |
| Capability to scale out the detection when the bandwidth/increase in future  |  |  |
| Capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and. hwp                               |  |  |
| Should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.   |  |  |
| Capability to export network packet files and encrypted suspicious files for further investigation.  |  |  |



|  |  |  |
|--|--|--|
| Capability to perform tracking and analysis of virus downloads and suspicious files  |  |  |
| Support exporting of analysis results such as Command and Control (C&C) server IP and malicious domain listing   |  |  |
| Capability to scan inside password protected archives  |  |  |
| Capability to detect malwares and spywares on Windows and non-Windows platforms.   |  |  |
| Should have option to configure unrestricted internet for sandboxes  |  |  |
| Support local password authentication schemes  |  |  |
| Capability to configure files, IP, URLs and Domains to black list or white list  |  |  |
| Capability to detect Mac, Linux and mobile malwares  |  |  |
| Capability to include user-defined and context-derived passwords for protected archives  |  |  |
| Capability to configure separate notifications to the administrator or individuals based on specific events like, sandbox detection, black list and license events etc.                      |  |  |
| Able to detect known malwares before sending suspicious files to sandbox for analysis  |  |  |
| Able to correlate local Advanced Persistent Threat (APT) attacks with global historical APT attacks.   |  |  |
| Support at least 1 Gbps of throughput  |  |  |
| Should have two (2) x one (1) TB Hard disks  |  |  |
| Should support at least 5x10/100/1000 Ethernet Interfaces  |  |  |
| Capability to detect attacker behavior within the network like (hash dumping, Hash Validation, Data Extraction from Database servers, DNS queries to suspicious or known C&C Servers, etc..) |  |  |
| Able to detect malicious and suspicious behaviors during non-office hours  |  |  |
| Should have on box correlation of threats  |  |  |
| Support open Web Services API for 3rd party or scripting integration   |  |  |
| Support manual submission for analysis   |  |  |
| Able to identify suspicious embedded object in document file like Object Linking and embedding (OLE) & macro extraction, shellcode & exploit matching  |  |  |
| Able to detect malicious or malformed file zero-day detection and script embedding   |  |  |
| Able to detect and alert if file has suspicious attributes like true-file type, file extension & naming trick  |  |  |
| Support Microsoft Office 2016 application for Office file analysis in sandbox images   |  |  |

|   |  |  |
|---|--|--|
|   |  |  |
| <b><u>Report:</u></b>   |  |  |
| Should have an intuitive dashboard that offers real time threat visibility and attack characteristics.  |  |  |
| Should provide reports with (but not limited to) HTML/CSV/PDF formats   |  |  |
| Review detection details based on predefined smart filters  |  |  |
| Able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)                          |  |  |
| Support logging of important parameters like source IP, destination IP, ports, protocol, domain, time stamp etc. of the attacks sessions.   |  |  |
| Should have the flexibility to provide customizable dashboard.  |  |  |
| Should have the option to provide investigative dashboard that is capable of displaying correlated graphical data that is based on link-graph, geomap, chart, tree-map/pivot table. |  |  |
| Able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.          |  |  |
| Able to provide intelligence portal for malware information, threat profile and containment remediation recommendations where applicable  |  |  |
| Capability to configure separate notifications to the administrator or individuals based on specific events like, sandbox detection, black List and license events etc.             |  |  |
| Able to generate out of box reports to highlight Infections, C&C behavior, lateral moment, asset and data discovery and data exfiltration   |  |  |
| Ability to programmatically output sandbox detections in OpenIOC format   |  |  |
| Able to determine overall host vulnerability levels by mapping threats to threat lifecycle rules  |  |  |
| Able to provide details of prevalence, maturity of a given file   |  |  |
| Support remote administration using Secure Shell (SSH)/HTTP Secure (HTTPS)  |  |  |
| Support Command Line Interface (CLI), Graphical User Interface (GUI)/Web based Administration Console.  |  |  |
|   |  |  |
| <b><u>Support:</u></b>  |  |  |
| Should provide daily 8 by 5 phone, email, and remote support with critical level onsite assistance  |  |  |

|  |  |  |
|--|--|--|
| Should have access to high-level of support via the principal for critical level concerns  |  |  |
| Should provide professional implementation services  |  |  |
| Should provide an annual health check to ensure that the product is properly working   |  |  |
|  |  |  |
| <b><u>Recognition:</u></b>   |  |  |
| Recognized in the industry for breach detection and performance  |  |  |
|  |  |  |
| <b>Ten (10) licenses comprehensive security platform for physical, virtual, and cloud servers</b>  |  |  |
| <b><u>Intrusion Prevention:</u></b>  |  |  |
| Able to provide Hostbased Intrusion Detection System (HIDS)/Hostbased Intrusion Prevention System (HIPS) feature, agent and agentless  |  |  |
| Feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content deviations, content that signals an attack, or policy violations                                       |  |  |
| Able to operate in detection or prevention mode to protect operating systems and enterprise applications vulnerabilities   |  |  |
| Able to provide detailed events with valuable information, including identity of the attackers, when they attacked, and what they attempted to exploit; administrators should be notified automatically via alerts when an incident has occurred |  |  |
| Able to provide protection against known and zero-day attacks  |  |  |
| Protection can be pushed out to thousands of virtual desktops in minutes without a system reboot   |  |  |
| Includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services   |  |  |
| Smart rules to provide zero-day protection from unknown exploits that attack an unknown vulnerability, by detecting unusual protocol data containing malicious code  |  |  |
| Exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits   |  |  |
| Compliance (Payment Card Industry Data Security Standard [PCI DSS] 6.6) to protect web applications and the data they process  |  |  |

|   |  |   |
|---|--|---|
| Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot   |  |   |
| Must be able to provide Application Control on the network layer  |  |   |
|   |  |   |
| <b><u>Firewall Function:</u></b>  |  |   |
| Includes an enterprise-grade, bi-directional stateful firewall providing centralized management of firewall policy, including predefined templates  |  |   |
| Virtual Machine isolation   |  |   |
| Fine-grained filtering (IP and MAC addresses, ports)  |  |   |
| Coverage of all IP-based protocols (Transmission Control Protocol [TCP], User Datagram Protocol [UDP], Internet Control Message Protocol [ICMP], Gateway-to-Gateway Protocol [GGP], Internet Group Management Protocol [IGMP], etc) and all frame types (Internet Protocol [IP], Address Resolution Protocol [ARP], etc.) |  |   |
| Prevention of denial of service (DoS) attack  |  |   |
| Design policies per network interfaces  |  |   |
| Detection of reconnaissance scans   |  |   |
|   |  |   |
| <b><u>Anti Malware:</u></b>   |  |   |
| Able to avoid resource contention such as antivirus Strom in the virtualized VDI environment  |  |   |
| Able to provide Web reputation filtering to protect against malicious sites for virtual desktops  |  |   |
|   |  |   |
| <b><u>Log Inspection:</u></b>   |  |   |
| Able to provide the capability to inspect logs and events generated by operating systems and applications   |  |   |
| Able to automatically recommend and assign relevant log inspection rules to the server based on the operating system and applications installed   |  |   |
| Able to automatically recommend and unassign log inspections rules that are not required  |  |   |
| Comes with pre-defined template for operating system and enterprise applications to avoid manual creation of the rules  |  |   |
| Able to create customized rule to support custom application  |  |  |

|  |  |  |
|--|--|--|
|  |  |  |
| <b><u>Integrity Monitoring:</u></b>  |  |  |
| Able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes in real time                              |  |  |
|  |  |  |
| <b><u>Virtual Patching:</u></b>  |  |  |
| Provide virtual patching which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs within minutes |  |  |
| Vulnerability rules to shield known vulnerabilities from an unlimited number of exploits; automatically shields newly discovered vulnerable within hours   |  |  |
| Intelligence to provide recommended virtual patching rules to protect OS & applications  |  |  |
| Able to create scheduled tasks to run recommendation scan to discover new rules to apply   |  |  |
| Able to automatically assign new virtual patching rules through scheduled tasks  |  |  |
| Able to automatically unassign virtual patching rules after physical patch has been installed  |  |  |
|  |  |  |
| <b><u>Event Tagging:</u></b>   |  |  |
| Support event tagging so that Administrator can add "tag" to events generated by the solution  |  |  |
| Tag must be fully customizable; Administrators can add, edit, and delete their own tag with own name   |  |  |
| Able to search for events based on the "Tag"   |  |  |
| Allow administrator to specify a specific event that is to be automatically tagged by the system   |  |  |
|  |  |  |
| <b><u>Management Console:</u></b>  |  |  |
| Dashboard to display multiple information  |  |  |
| Dashboard must be configurable by administrator to display the required information only   |  |  |
| Web-based management system for administrators to access using web browsers  |  |  |

|   |  |  |
|---|--|--|
| "Alerts" on the main menu to view administrator notifications concerning system or security events  |  |  |
| Firewall events to view activities on computers with the firewall enabled (typically includes dropped or logged packets)  |  |  |
| Access to Deep Packet Inspection (DPI) events to view security-related DPI activities; this section should display exploits detected, either resulting in dropped traffic (Prevent Mode) or logging of events (Detect Mode) |  |  |
| System events to view a summary of security-related events, primarily for the management server and also including agents' system events; all administrative actions should be audited with the system events               |  |  |
|   |  |  |
| <b><u>Compliance and Certifications:</u></b>  |  |  |
| Must provide support for:   |  |  |
| National Institute of Standards and Technology (NIST)   |  |  |
| Health Insurance Portability and Accountability Act (HIPAA)   |  |  |
| Sarbanes-Oxley Act (SOX)  |  |  |
| Basel2  |  |  |
| ISO 2700x   |  |  |
| Statement on Auditing Standards (SAS) 70  |  |  |
| Data Privacy Act (DPA)  |  |  |
| Must be certified to common Criteria EAL4+  |  |  |
| Must be certified by EMC VSPEX  |  |  |
| Must be validated for Cisco UCS   |  |  |
| Must be validated for NetAPP flexpod  |  |  |
|   |  |  |
| <b><u>Other Requirements:</u></b>   |  |  |
| Able to integrate to a SIEM   |  |  |
| Directory integration for enterprise directories including Microsoft Active Directory   |  |  |
| Support selective module on agent installation  |  |  |
| Knowledge transfer training   |  |  |
|   |  |  |

*Handwritten initials/signature*

|  |   |  |  |
|--|---|--|--|
|  | <b><u>Support:</u></b>  |  |  |
|  | Support with onsite assistance from a local source  |  |  |
|  | Provide 24x7 support via email/call   |  |  |
|  | Provide direct support for installation and upgrade                                       |  |  |
|  | Security assessment and recommendation should be provided every 6 months                  |  |  |
|  |   |  |  |
|  | <b><u>Inclusions:</u></b>   |  |  |
|  | Implementation and support services for one (1) year license subscription                 |  |  |
|  | 2 days knowledge transfer training for 2 pax.   |  |  |
|  | Able to integrate with existing security suite  |  |  |
|  | Installation and configuration shall be carried out on an existing Hyper-V MS 2012 server |  |  |
|  | Implement the project in 30 working days  |  |  |

**Bidder's Authorized Representative:**

\_\_\_\_\_  
**Signature over Printed Name**

\_\_\_\_\_  
**Principal Bidder / Supplier**

11

*Section VIII. Checklist of Requirements for  
Bidders*

Uncontrolled when printed or emailed





# Checklist of Requirements for Bidders

**"EACH AND EVERY PAGE OF THE BID FORM, INCLUDING THE SCHEDULE OF PRICES, UNDER SECTION IX HEREOF, SHALL BE SIGNED BY THE DULY AUTHORIZED REPRESENTATIVE/S OF THE BIDDER. FAILURE TO DO SO SHALL BE A GROUND FOR THE REJECTION OF THE BID AND PROPERLY TABBED AS FOLLOWS:"**

## ELIGIBILITY DOCUMENTS' ENVELOPE

- Tab A** PhilGEPS Certificate of Registration under Platinum Membership
- Tab B** Notarized Omnibus Sworn Statement/Affidavit of the prospective bidder (of its background, affiliations, responsibilities as Bidder, authorizations, etc.) (**Section IX, Bidding Forms**)
- Tab C** Statement / List of **all on-going, and completed** government and private contracts, similar in nature to the contract/project subject of the bidding at hand, within at least the past **three (3) years** (December 2015 to December 2018) using the following forms and support documents:
- (FORM SF-GOOD-13a) Statement 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.
  - (FORM SF-GOOD-13b) Statement / List of at least one (1) **COMPLETED** government and/or private contracts (**Section IX, Bidding Forms**) similar in nature as the contract subject of bidding with a value of at least fifty (50%) of the Approved Budget for the Contract (ABC); or two (2) similar contracts with the aggregate contract amount equivalent to at least fifty percent (50%) of the ABC of the contract subject of bidding at hand supported with the following documents (in accordance to BDS Clause 5.4 of the BDS):
    1. Purchase Order or Contract; **AND**
    2. Certificate of Completion or Official Receipt of last payment received
- Tab D** Computation of Net Financial Contracting Capacity (NFCC) in accordance with ITB Clause 5 (**Section IX, Bidding Forms**)
- Tab E** Bid Security (use **Section IX, Bidding Forms** in case of Bid Securing Declaration)



**Tab F** Technical Specifications Compliance Form (Use the supplied Technical Specifications Compliance Form found in the Bid Documents as Tab H)

**Tab G** Schedule of Requirements (*use Section VI*) duly signed in every page by the principal bidder or the bidder's authorized representative

**Tab H** Valid Joint Venture Agreement (JVA) in case the joint venture is already in existence. In the absence of a JVA, 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 shall be included in the bid.

Additional documents for Joint Venture

Further, each partner of the JV shall likewise submit the following requirements consistent with ITB Clause 12.1.(a)(i) and 12.1.(a)(ii):

- 12.1.(a)(i) Registration certificate from the Securities and Exchange Commission (SEC) for corporation, Department of Trade and Industry (DTI) for sole proprietorship, or Cooperative Development Authority (CDA) for Cooperatives; and
- 12.1.(a)(ii) Valid Mayor's permit issued by the city or municipality where the principal place of business of the prospective bidder is located.

Submission of the following documents consistent with ITB Clause 12.1.(a)(iii) to 12.1.(a)(v) by any of the joint venture partners constitute compliance:

- 12.1.(a)(iii) Statement of ongoing and completed government and/or private contracts within at least the past three (3) years following item 2 above
- 12.1.(a)(iv) Audited Financial Statements for 2017, stamped "Received" by the Bureau of Internal Revenue (BIR) or its duly accredited and authorized institutions; and
- 12.1.(a)(v) Computation of Net Financial Contracting Capacity (NFCC) in accordance with ITB Clause 5.5. ;

**FINANCIAL PROPOSAL ENVELOPE**

The Financial Component shall contain the following:

**Tab I** Financial Bid Form (*use Section IX Bidding Forms*)



***Section IX. Bidding Forms***

Uncontrolled when printed or emailed

## TABLE OF CONTENTS

|   |           |
|---|-----------|
| BID FORM .....  | 71        |
| OMNIBUS SWORN STATEMENT .....   | 73        |
| BID SECURING DECLARATION FORM .....   | 76        |
| STATEMENT / LIST OF ALL ONGOING GOVERNMENT & PRIVATE<br>CONTRACTS INCLUDING CONTRACTS AWARDED BUT NOT YET STARTED ..... | <u>78</u> |
| STATEMENT / LIST OF ALL ONGOING GOVERNMENT & PRIVATE<br>CONTRACTS COMPLETED WHICH ARE SIMILAR IN NATURE .....           | <u>79</u> |
| FINANCIAL DOCUMENTS FOR ELIGIBILITY CHECK .....   | <u>80</u> |

Uncontrolled when printed or emailed

