ANNEX A

PROJECT: Supply, Delivery and Installation into Operational Integrated Security Monitoring Solution

A. Issues raised during the Pre-bid Conference

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
1.	1) Can you consider cloud-based solution for the project.	1) No, only On-premise solution.
2.	2) Request for the following information. a) MPS b) Threads per second c) Inventory of Sources d) Scope of Work	2) As requested: a) Messages Per Second b) No of users/requests/processes per second c) See Attachment A d) Refer to page 66, Section VII. Technical Specifications Item 6.1.
3.	3) The published Bid Form format is different from what was presented during the Pre-Bid Conference.	3) Revisions will be applied to the new Bid Form and will be included to the Bid Bulletin.
4.	4) Can you consider a different hardware specifications but will still comply with the minimum requirements?	4) Yes
5.	5) On SLCC, the published track record requirement is different from what was presented. Five (5) years as published but four (4) years during presentation.	5) Five (5) years.

B. REPLY TO WRITTEN QUERIES/CLARIFICATIONS

WRITTEN CLARIFICATIONS / ISSUES / QUERIES

I. INFOBAHN COMMUNICATIONS, INC.

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
6.	6) List of Log Sources or inventory (Detailed as possible: OS, Version, Brand name and Sites where the Log Sources is residing in)	6) See Attachment A.
7.	7) How many Sites?	7) One (1)
8.	8) Can we exceed to the minimum hardware specs? (Though it was already answered in the pre-bid earlier that we can based it on the specs of LogRhythm just to put into writing)	8) Yes
9.	9) How deep is the need for Threat Intelligence? Does your agency needs a full blown TI or the Free TI of LogRhythm will suffice?	9) We need deeper and full blown Threat Intelligence not a Freeware TI
10.	10) Please explain the requirements for User Behavioral Analytics in their "Additional Requirement" section in the RFP.	10) Please refer to page 59, Item 1.6.1 Section VII. Technical Specifications.
11.	11) Explain "System wide" does this mean it will be implemented nationwide and all the Log Source will be fed to the main site or the requirement will only be applied to the main site? Considering that only 15m php budget is allocated for this project?	11) All log sources will only be applied to the main office site but the servers in the main office are connected to all branches nationwide.

II. NERA PHILIPPINES, INC.

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
12.	1) Does the agency have an existing Integrated Security Monitoring Solution?	1) None
13.	2) Does the agency require Managed Security Services (MSS) after the installation and commission of the	2) No

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
	Integrated Security Monitoring Solution?	
14.	3) What is the estimated total number of events per second?	3) 10,000 events per second
15.	4) What is the projected growth rate in percentage (%) in 3 to 5 year time?	4) 30%
16.	5) Logs and events would be collected from which systems, applications and security devices?	5) See Attachment A.
17.	6) What are the functionality of these systems, applications and security devices?	6) See Attachment A.
18.	7) Logs and events would be collected from the how many locations/branches?	7) Only from the Main Office
19.	8) Is it possible to provide us with a high level network diagram? Together with the different locations/branches (if any)	8) High level network diagram will be provided to the winning bidder.
20.	9) Is HA (High Availability) required?	9) No
21.	10) What is the tolerance level for downtime?	10) 0.01%
22.	11) With regards to the Single Largest Completed Contract, since your agency's requirement fall on Security Solutions. We would like to clarify if we can submit or comply this requirement by submitting any project or documents related to "Supply, Delivery, Installation, Configuration of Security Solution"?	11) The following are the acceptable Security Solutions or combination of any or all of the following: - Security Information and Events Management (SIEM) - Log Management - Endpoint Security - Firewalls - Intrusion Prevention and Detection ***This amends Section III, Item 5.4 on page 27 of the Bid Document***

III. ACCENT MICRO TECHNOLOGIES, INC.

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
	TECHNICAL SPECIFICATIONS (Section VII. Technical Specifications, pages 55 to 67)	
23.	1) Page **55** Item **1.1.1**: - Policy-based incident notification framework. What is SSS current notification framework?	1) We have no current/existing SIEM
24.	2) Page **55** Item **1.2.2**: - Must be able to use business service parameters that prioritizes alerts from a business service perspective. Will business rules be available and provided as needed?	2) Yes, business rules will be provided to the winning bidder.
25.	3) Page **55** Item **1.2.3**: - Must support Historical Search feature which can retrieve events from the event database. By using either a simple keyword-based search or a more detailed structured search, can get quick and valuable insights into events that have occurred over any selected time period. Retention period for historical search?	3) At least one (1) year
26.	4) Page **55** Item **1.2.4**: - Must support creation of custom parsers for device logs that involves writing an XML specification for the parser, and then using a test event to make sure the logs are parsed correctly. It is possible to use regex (regular expression) for the parsing of data?	4) Yes
27.	5) Page **56** Item **1.2.5**: - Must be able to correlate event and flow data from different vendor products into a normalized event taxonomy to make it possible to detect larger incidents. What are the different vendor products that will be integrated?	5) Checkpoint, Fortinet, Symantec, Cisco, Mcafee, BeyondTrust, Gemalto, Riverbed, Network Access Control

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
		Solution, Network and Oracle Identity Manager
28.	6) Page **56** Item **1.3.4**: - Must perform monitoring and analysis of data from a broad heterogeneous security infrastructure and offer two-way integration via open interfaces. Must allow automated first response actions. Current security infrastructure?	6) Will be provided to the winning bidder
29.	7) Page **56** Item **1.3.5**: - Must provide security team complete and correlated access to the content and context needed for fast, risk-based decisions. How many concurrent users? Is it going to be connected to a directory service infra (AD)?	7) 8,000 internal users. 20 Security Admin No AD (Active Directory).
30.	8) Page **56** Item **1.3.6**: - Must provide integrated tools for configuration and change management, case management, and centralized policy management. Kindly specify what is meant by "centralized Policy management". Does it refer to correlation rules management?	8) Centralized Policy Management means a system management tool that will centrally manage/administer the policy, reports, correlation rules, alerts, users, etc.,
31.	9) Page **56** Item **1.3.8**: - Must be able to collect, process, and correlate log events from multiple years with other data streams, including STIX based threat intelligence feeds, depending on user speed requirement. Retention period?	9) At least one (1) year
32.	10) Page **56** Item **1.3.9**: - Must be able to store billions of events and flows, allowing all information to be available for immediate ad hoc queries, forensics, rules validation, and compliance.	10) At least one (1) year

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
	Retention period?	
33.	11) Page **56** Item **1.3.11**: • Must enable collection of more information from more sources through scalability and performance. Information may include application content such as documents, transactions, and communications, providing deep forensic value to the user. The information must be heavily indexed, normalized, and correlated to detect a wider range of risks and threats. Are these documents/transactions in a flat file format? How are we going to get these data? Mode of transfer?	11) Yes, flat file data Method or process of getting data will be solution-based. It depends on your product's functionality or scripting capability on how to comply with this item.
34.	12) Page **56** Item **1.3.12**: • Must calculate baseline activity for all collected information and provide prioritized alerts with goal of discovering potential threats before occurrence. Must perform analysis for data patterns that may indicate larger threats. Do you have endpoints? Anti-virus? Intrusion detection/prevention tool? Firewall?	12) Yes, we have endpoints, anti-virus, IPS,IDS and Firewall

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
35.	13) Page **57** Item **1.3.15**: - Must support out of the box, ready to be used and customizable generation of hundreds of reports, views, rules, and alerts. What are you looking to get out from the solution? Visualizations/reports already in mind?	13) We are looking for a solution that is capable of generating customized reports that may be defined by the user in addition to the already available or canned report templates.
36.	14) Page **57** Item **1.3.16**: - Must enable easy visualization, investigation, and reporting on the most relevant security information.. What are you looking to get out from the solution? Visualizations/reports already in mind?	14) We are looking for a solution that is capable of generating customized reports that may be defined by the user in addition to the already available or canned report templates.
37.	15) Page **57** Item **1.4.2**:: - Must be able to collect security events and network flow data from hundreds of third-party sources. What are these third party sources?	15) Third-party sources refers to products that are not in same brand/family as the offered solution.
38.	16) Page **57** Item **1.4.3**:: - Must automate log management and analysis for all log types, including Microsoft Windows event logs, database logs, application logs and syslogs. Do you have other logs that are not stated in the TOR?	16) None
39.	17) Page **57** Item **1.4.5**:: - Must provide and support out-of-the-box compliance rule sets and reports Will the rule sets and reports be provided?	17) Yes.
40.	18) Page **57** Item **1.4.6**:: - Must utilize tightly integrated log	

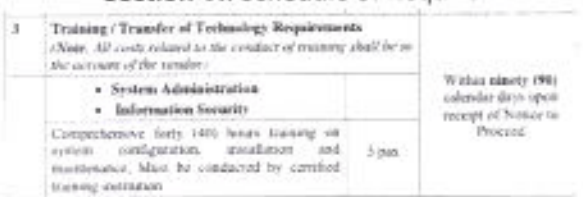
ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
	collection, management, and analysis environment to strengthen security profile and improve user ability to comply with standards such as PCIDSS, HIPAA, NERCCIP, FISMA, GLBA, and SOX. Can an agent be installed where the logs reside?	18) Yes, agents may be installed in the log sources
41.	19) Page **57** Item **1.4.7**:: - Must be able to scale appliances to tens of thousands of events per second, providing dedicated, reliable collection for distributed sources. Events per second of each data source?	19) See Attachment A
42.	20) Page **57** Item **1.4.8**:: - Must be able to cache locally all collected data to preserve data in the event of network communication error or outage. High availability or disaster recovery? Is data replication required? Does it need to be searchable at all time?	20) No High Availability nor Disaster Recovery. No data replication required Yes
43.	21) Page **58,** Item **1.5.1**:: - Must immediately detect nodes on user network when communicating with a suspicious or known bad actor and quickly understands the threat's path. Can list of valid IP's on the network be provided as need?	21) Yes
44.	22) Page **58,** Item **1.5.6**:: - Must allow seamless integration of Threat intelligence with security manager alarm and other alerting mechanisms, to ensure interactions with known malicious systems. What are the current security manager alarms and other alerting mechanism?	22) Email

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
45.	23) Page **58,** Item **1.5.7**:: - Must automatically receive and process new source reputations in security manager. What are the current security manager alarms and other alerting mechanism?	23) Email
46.	24) Page **59,** Item **1.5.9**:: - Must be able to quickly identify attack paths and past interactions with known bad actors associated with botnet/ distributed denial-of-service (DDoS), mail/spam-sending malware that hosts network probing, malware presence, DNS hosting, and activity generated by intrusion attacks. Are these devices available to be integrated to the solution?	24) Yes, the proposed solution must be able to integrate with the existing security solutions in ATTACHMENT A
47.	25) Page **59,** Item **1.6.3**:: - Must support scheduled reporting and result delivery via 1 email. Is email server credential available?	25) Yes, will provided to the winning bidder when needed
48.	26) Page **59,** Item **1.6.8**:: - Must be integrated with load-balancing architecture for collecting events from remote sites. Can you provide the logging environment (diagram)?	26) Yes, will be provided to the winning bidder
	OTHER TECHNICAL QUESTIIONS	
49.	27) What are the different devices to be integrated to the solution? Their brand and quantities?	27) See Attachment A
50.	28) Log formats of each data?	28) Text format
51.	29) Do we have the inventory of the devices for proper scoping?	29) See Attachment A
52.	30) Events per second of each data?	30) See Attachment A
53.	31) Retention period of each data?	31) At least 1 year

ITEM NO.	QUERIES/CLARIFICATIONS	SSS RESPONSE
54.	32) Levels of access? Who are going to access each data?	32) Security, Infrastructure and Monitoring Teams

IV. **TRENDS AND TECHNOLOGIES, INC.**

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
55.	1) Page **27,** Item **5.4**:: - The Bidder must have completed, within five (5) years prior to the deadline for submission and opening of bids, a single contract that is similar to this Project, equivalent to at least fifty percent (50%) of the ABC. - For this purpose, similar contracts shall refer to Installation and Implementation of Integrated Security Monitoring Solution or equivalent Information and Event Management Implementation **1.1.** *As option, can you also consider Intrusion Prevention System (IPS) or combination of Perimeter Firewall and Intrusion Prevention System (IPS)?*	**1.1** Yes. Intrusion Prevention System and Perimeter Firewall or combination of both are acceptable
56.	2) Page **51,** Item **16.1**:: **A. DURING POST QUALIFICATION** - The bidder being evaluated must provide reference site or deliver and install the demo hardware and software to the SSS Main Office within the period specified by BAC to enable the TWG to test the following • Proposed solution's functionalities and features • Compatibility and integration capability with the intended application - The cost, if any, of the hardware and the software during the post-qualification shall be to the account of the vendor. **2.1.** *One of the option is to install demo hardware and software, can we use a demo system on Virtualization Machine (VM) environment?* **2.2.** *Aside from reference site or deliver and install the demo hardware and software,*	**2.1.** Yes, demo system on Virtualization Machine (VM) environment is acceptable. **2.2.** No.

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
	can you also consider principal's web base lab demo?	
57.	3) Page **54,** Item **16.1**:: **Section VI.** Schedule of Requirement  3 **Training / Transfer of Technology Requirements** *(Note: All costs related to the conduct of training shall be to the account of the vendor)* • **System Administration** • **Information Security** Comprehensive forty 140) hours training on system configuration, installation and maintenance, Must be conducted by certified training institution 5 pax Within **ninety (90)** calendar days upon receipt of Notice to Proceed - Training / Transfer of Technology. . System Administration . Information Security ***3.1.** Is this System administration only?* Page **61,** Item **3.3**: **Section VII.** Technical Specification - Information Security Training shall be conducted in a Training Center (classroom type) by a certified training instructor. Bidder must submit a proof that the training instructor is affiliated or member of a certified training institution that is recognized globally to conduct certification exam. **3.2.** *Is this needed or System Administration Training only?*	**3.1.** Yes. For System Administration only. **3.2.** This is applicable for Information Security
58.	4) Page **60,** Item **1**:: Certification - Certificate from the manufacturer ***4.1.** As option, can this be from a local Distributor?*	**4.1.** Yes
59.	5) Page **56,** Item **1.3.1**:: . Must support at least 1 year correlated log retention. **5.1.** *What is the recommended Events Per Second (EPS) requirement?* *In line with this question, will there be any expansion after the 3 years? Hence, please include this in your EPS requirement.*	5.1 10,000 events per second is the EPS requirement and should be doubled in 3 years.

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
	5.2. *Where and what are the devices needed to be logged by SIEM?*	5.2 See Attachment A
60.	6) Page **57,** Item **1.3.17**:: - Must support integration with the Unified Compliance Framework (UCF), that enables a "collect-once, comply with- many" methodology for meeting compliance requirements and keeping audit efforts and expense to a minimum. **6.1.** *For Unified Compliance Framework (UCF), we have equivalent technology. We have unified search framework that can be used on dashboard and reports, which can achieve the same objective. Can we proposed this instead?*	**6.1.**Yes
61.	7) Page **59,** Item **1.7.3**: - **36TB** **7.1.** *Since this is solution based requirement, can we comply with the 36TB server specification if we distribute the specs across the different server that we will use?* *Do we still need to provide 30 units of Bluetooth USB dongle?*	**7.1.**Yes you can use other server types as long as you can comply with the 36TB. No, we are not requiring *"30 units of Bluetooth USB dongle?" For clarification,* we mean the following USB ports 2 x USB 2.0; **2 x USB 3.0**
62.	8) *Since we are planning participate on the Acquisition of Network of Equipment which has the same date of bid submission and bid opening, we humbly appeal for a 2 weeks extension on the bid submission and opening. The extension will give us enough time to prepare all submittals on all bids. Furthermore, the extension will give all the vendors enough time to prepare for the POC criteria requirement*	C/O BAC
	Other Clarifications	
1.	Section V, Item 11.3 is hereby amended to: The terms of payment shall be in accordance with the schedule as stipulated in the Bid	

ITEM NO.	QUERIES/CLARIFICATIONS	TWG RESPONSE
	Proposal on page 71 of this document. This amends Section V, Item 11.3 on page 51 of the Bid Document	
2.	Attachment B: Revised Bid Breakdown which amends Bid breakdown on page 71 of the Bid Document	

ATTACHMENT A. SIEM SCOPING

Log Sources	Brand Name	OS Version	Events/Connection per Second	Location
1. Enterprise Firewall	Checkpoint NGX	R77.30	2,260/second	Main Office
2. Web Application Firewall	Fortiweb	FortiWeb-4000D 5.86,build1413,171204	565/second	Main Office
3. End-Point Security Solution	Symantec	Windows Server 2012 R2 Standard	353/second	Main Office
4. Internal Firewall	Fortinet	Fortigate 5.6	Newly Acquired	Main Office
5. Information Systems Security Solution (ISSS)	Gemalto	Windows Server 2016 Standard	Newly Acquired	Main Office
	Mcafee	Windows Server 2016 Standard	Newly Acquired	Main Office
	BeyondTrust	BEYONDINSIGHT 6.8.0.192	Newly Acquired	Main Office
6. Others	Network Equipment			Main Office

ATTACHMENT B. REVISED BID BREAKDOWN

A. Bid Breakdown

Name of Bidder _____ Invitation to Bid No. _____

Page _____ of _____

Cost Component (Note: Include all applicable components)	Year 1	Year 2	Year 3	Year 4	Year 5	TOTAL
Integrated Security Solution						
1. Hardware / Software Cost (Itemize)	₱	₱	₱	₱	₱	₱
2. Other Requirements (itemize)	₱	₱	₱	₱	₱	₱
3. Transfer of Technology/Training	FREE					
4. Two-year Warranty and Maintenance	FREE		N/A	N/A	N/A	0
5. Three-year Maintenance after the warranty period	N/A	N/A	₱	₱	₱	₱
6. Delivery and Installation, if applicable (Itemize)	₱	N/A	N/A	N/A	N/A	₱
TOTAL	₱	₱	₱	₱	₱	₱

Note:

1. Fill up all required items/field in the bid breakdown. **Failure to indicate any of the following shall mean outright disqualification** since bid is considered Non-Responsive per Section II. Instruction to Bidders, Items 15.2 and 28.3:
   - If the item is given for free, indicate dash (-), zero (0) or free
   - If the item is not applicable, indicate N/A
2. 3-year maintenance costs must be distributed equally over 3 years.
3. All documents shall be signed, and each and every page thereof shall be initialed by the duly authorized representative/s of the Bidder per Section II. Instruction to Bidders, Item 19.4.
4. Warranty requirement is at no cost to SSS.
5. The total bid shall not exceed the ABC.