SPECIAL BIDS AND AWARDS COMMITTEE FOR THE INTEGRATED GOVERNMENT PHILIPPINES PROJECT (BAC4IGOV)

Supplemental Bid Bulletin No. 5

NATIONAL GOVERNMENT DATA CENTER 1 (NGDC1)
NETWORK SECURITY SOLUTIONS PROJECT

Bid Reference No. BAC4IGOV-2017-03-001

Please be advised of the changes in the schedule of the Submission and Opening of Bids for this project:

ACTIVITY	PREVIOUS SCCHEDULE	REVISED SCHEDULE
Submission of Bids	10 May 2017 10:00 AM	16 May 2017 10:00 AM
Opening of Bids	10 May 2017 11:00 AM	16 May 2017 11:00 AM

Please use the **Revised Reference Table of Bid Compliance as of 9 May 2017** attached in this Supplemental Bid Bulletin. (Note: Bidders who bought the bidding documents will be provided with the Excel file of this form.)

All terms, conditions and instructions to bidders specified in the Bidding Documents inconsistent with this Bid Bulletin are hereby superseded and modified accordingly.

For information and guidance of all concerned.

Issued this 9th day of May 2017.

(Original Signed)
ALONA H. ISIDRO
Vice Chairperson, BAC4IGOV

NATIONAL GOVERNMENT DATA CENTER 1 (NGDC1)
NETWORK SECURITY SOLUTIONS PROJECT

Bid Reference No. BAC4IGOV-2017-03-001

REVISED REFERENCE TABLE OF BID COMPLIANCE AS OF 9 MAY 2017

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
1.0	**ADVANCED THREAT PROTECTION**	
1.1	**SSL VISIBILITY**	
1.1.1	Automatically identifies all SSL/TLS traffic regardless of port number or application	
1.1.2	Uncovers hidden threats that use SSL to bypass detection, such as the Dyre and Zeus trojans,	
1.1.3	Upatre Command and Control (C&C), VMZeus C&C, etc.	
1.1.4	Selectively decrypts traffic to meet data privacy and compliance requirements	
1.1.5	Enforces acceptable use policies for encrypted traffic	
1.1.6	Line rate network performance that can send non-SSL flows to the attached security appliance(s) or cut-through in less than 40 microseconds to minimize any delay for latency sensitive applications, such as Voice over IP (VoIP)	
1.1.7	Supports decryption of up to 9 Gbps of SSL traffic for all SSL/TLS versions and over 70 cipher suites.	
1.1.8	High Connection Rate/Flow Count that can inspect up to 800,000 concurrent SSL sessions and supporting the teardown and setup of up to 30,000 new sessions per second	
1.1.9	Has integrated fail-to-wire/fail-to-open hardware and configurable link state monitoring and mirroring for guaranteed network availability and network security	
1.1.10	Capable of Input Aggregation to allow aggregation of traffic from multiple network taps onto a single passive-tap segment for inspection.	
1.1.11	SSL-secured, simple-to-use, web-based user interface (UI) for con guration and management.	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
1.1.12	Centralized Management that allows multiple appliances to be administered including inventory and RBAC System performance monitoring, health monitoring, configuration backup and scheduling and configuration synchronization.	
1.1.13	E-mail Alerting on configured logs to trigger alerts that can be immediately forwarded via email or sent at intervals to designated network administrators.	
1.1.14	SSL Session Identification to provide session logs details of all SSL flows, inspected or not, allowing suspicious trends or patterns of SSL use to be detected	
1.1.15	Supports up to 8 remote syslog servers to enable enhanced reporting and logging applications within distributed environments.	
1.1.16	Has complete visibility into inbound and outbound SSL sessions	
1.1.17	supports networks with asymmetric traffic routing	
1.1.18	support for multiple re-signing Certi cate Authorities (CA) when inspecting outbound SSL flows	
1.2	**ADVANCED SECURITY GATEWAY**	
1.2.1	The proxy appliance shall be in Gartner Magic Quadrant, NSS Labs, IDC and/or Forrester for Secure Web Gateway.	
1.2.2	The proxy appliance shall be an appliance based solution; with a thin OS single purpose operating system designed for secure proxy services.	
1.2.3	The proxy appliance shall support optional AV scanning engine within the same hardware appliance	
1.2.4	The proxy appliance shall not be based on Windows NT, Novell Netware, or any Unix variants.	
1.2.5	The proxy appliance shall support multiple bootable copies of the OS.	
1.2.6	The proxy appliance shall be able to operate multiple disk failures.	
1.2.7	The proxy appliance shall support the following authentication methods: NTLM, Active Directory, LDAP, RADIUS, CoreID, Local password database, Forms Authentication, Certificate Authentication, SAML Authentication, Policy Substitution	
1.2.8	The proxy appliance shall support realm sequences and multiple	

ITEM		SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
		authentication realms	
1.2.9		The proxy appliance shall support SSH and CLI	
1.2.10		The proxy appliance shall support transparent redirection of traffic from Layer 4 switches.	
1.2.11		The proxy appliance shall support ability to perform RDNS lookup for content filter database that does not have list of pre-resolved IP address.	
1.2.12		The proxy appliance shall support the following proxy protocols: HTTP 1.0, 1.1, TLS1.1, 1.2, FTP, DNS, SSL Forward Proxy, HTTPS Tunneling, HTTPS Termination, SOCKS v4 & v5, MMS, RTSP, RTMP, RTMPE, QuickTime, CIFS, MAPI and TCP Tunnel	
1.2.13		The content filter services shall support minimally 80 categories that includes: Malicious Outbound Data/Botnets , Malicious Sources/Malnets, Phishing, Suspicious, etc	
1.2.14		The proxy appliance shall support ability to control by protocols like FTP, HTTP, HTTPS and DNS.	
1.2.15		The proxy appliance shall support method level control for HTTP, HTTPS, FTP & SOCKS. Examples are as follows: GET, PUT, POST, LINK, UNLINK, CONNECT, etc for HTTP; DIR, LS, CD, MPUT, etc for FTP	
1.2.16		The proxy appliance shall support ability to filter by: File Extension, HTTP MIME Type	
1.2.17		The proxy appliance shall support the ability to perform True File Type detection (eg where a malicious external party may rename an executable as a jpeg file to bypass security filters)	
1.2.18		The proxy appliance shall support ability to strip-off active content like java applets, visual basic and java scripts as these objects have a high potential for malicious activity.	
1.2.19		The proxy appliance shall support ability to perform RDNS lookup for content filter database that does not have list of pre-resolved IP address.	
1.2.20		The proposed solution shall support a minimum choice of 3 commercial Anti-Virus engines.	
1.2.21		The proposed solution shall support AV vendors from Gartner Magic Quadrant, NSS Labs, IDC and/or Forrester	
1.2.22		The proposed solution shall have the ability to scan traffic with dual AV engines concurrently	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
1.2.23	The proposed solutions shall have a minimum of 1 billion entries for file whitelist database	
1.2.24	The proposed AV threat detection engines supported shall have the following capabilities: Checksum signature matching for known threats Command and content behavioral analysis for proactive detection Emulation mode for deep script analysis Executable analysis	
1.2.25	The proposed solution must have the ability to: Detect Spyware/Adware Perform Anti-virus engine heuristic Detect Potentially Unwanted Applications (adware) Detect True File Type/Apparent Data Type	
1.2.26	The proposed solution must be able to scan, block or ignore the following files archives: MS CAB archive file (.cab) ZIP archive file (.zip) Multi-part ZIP archive file (.zip.XXX) RAR archive file (.rar) Multi-part RAR archive file (.partX.rar) TAR archive file (.tar) GZIP compressed file (.gz, .tgz, .gzip) BZip2 archive file (.bz2, .tbz2) Flash files Shockwave Flash file, v1-v4 (.swf) Shockwave Flash file, v5+ (.swf) Flash video file (.flv)	
1.3	**SECURITY ANALYTICS (64Mbps with at least 15 days online retention)**	
1.3.1	Real-time threat intelligence, security analytics, and complete security visibility from the data center to remote of ces	
1.3.2	High performance and optimized storage to meet growing network traffic demands	
1.3.3	Integration with existing security infrastructure to leverage investments and established processes and workflows	
1.3.4	Layer 2-7 traffic capture and deep packet inspection	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
1.3.5	Provides a variety of analytics tools such as complete session reconstruction, data visualization, Root Cause Explorer, timeline analysis, file and object reconstruction, IP geolocation, and trend analysis.	
1.3.6	Can integrate with best-of-breed security technologies to pivot directly from any alert or log and obtain full-payload detail and evidence of the full source and scope of the event – before, during and after the breach	
1.3.7	Incident responder tool to extract network objects to reconstruct a timeline of suspect web sessions, emails, and chat conversation	
1.3.8	High performance with 2-10 Gbps interfaces for lossless capture on certied, industry- standard hardware platforms	
1.3.9	support for 6-20 TB on each appliance and add-on capacity to meet fast-changing requirements	
1.3.10	Centralized management so you can monitor thousands of network segments from a single pane of glass	
1.3.11	Access to the latest threat intelligence via internal threat blades and Global Threat feeds	
1.3.12	Large storage capacity to accommodate extended historical capture windows, up to 145TB usable storage	
1.4	**SANDBOXING APPLIANCE**	
1.4.1	A bare metal environment that emulates an actual system to detect malware that otherwise will not detonate in a virtualized environment	
1.4.2	Unique dual detection approach combines sandboxing with Intelligent Virtual Machines	
1.4.3	Virtual machine profiles that replicate actual production environments, including custom applications, to quickly spot anomalies and differences in behavior that unveil anti-analysis and other advanced malware evasion techniques	
1.4.4	Automatic sample classification and risk scoring by highest matched pattern along with support for existing malware analysis workflows	
1.4.5	Real-time incident reporting with detailed analysis of the event that provides immediate notification to security analysts	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
1.4.6	Has a web-based dashboard that enables easy searches of the malware intelligence and collection database, store samples, reports, and events.	
1.4.7	Process hundreds of thousands of files per day with parallel sample processing on up to 55 virtual machines per single Appliance	
1.4.8	Multiple VMs with Windows XP and Windows 7 OS's and unlimited software configurations can be supported.	
2.0	**NEXT GENERATION ENDPOINT (1,200 endpoints)(mixed servers and workstation)**	
2.1	**APPLICATION WHITELISTING SOLUTION**	
2.1.1	Endpoint agent should run in kernel mode	
2.1.2	Support for Windows, Linux and Mac	
2.1.3	Solution must scale to 50,000+ machines on one server	
2.1.4	Automatic maintainance of whitelist approvals by: By Directory By User By UNC Path By Digital Certificate By Process By Automatic Updater By Package	
2.1.5	Application Whitelisting to block Malicious software (spyware, adware, malware) and all software outside the defined list	
2.1.6	A single console that provides instant visibility into the files, executions and critical system resources on every machine to increase security posture by showing what has arrived and executed on every system in real-time and provide relevant actions to the events in real-time	
2.1.7	Visibility & protection in Real-time, both on corporate as well as off corporate network.	
2.1.8	Prevention of new and unknown software (greylist)	
2.1.9	Blocking of user-installed software, including privileged users	
2.1.10	Authorization of centrally deployed software	
2.1.11	Can control files or directories from being changed except by trusted processes without additional licenses	

ITEM		SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
2.1.12		Should have Advanced Threat Indicators to be able to identify unusual activities on the system and report them	
2.1.13		Monitor and/or protect registry elements from being changed by unauthorized sources	
2.1.14		Monitor and/or protect process memory space from being accessed or changed by unauthorized sources	
2.1.15		Should be able to identify the software as soon as it is introduced into the environment, not when it is executed	
2.1.16		Once software has been identified as arriving within our network, assistance is needed to determine what it is and where it came from	
2.1.17		The most useful and secure application of a whitelist product is strict enforcement of the whitelist, or lockdown	
2.1.18		For departments or groups where strict lockdown or high enforcement is not feasible, other more flexible enforcement levels should be available	
2.1.19		Even though certain groups are in flexible enforcement levels, the ability to block software based on a ban or blacklist is required	
2.1.20		The solution should provide a replacement for AV that will satisfy the PCI DSS Control 5	
2.1.21		The solution should satisfy PCI DSS Control 10.5 to Protect Log Data	
2.1.22		The solution should satisfy PCI DSS Control 11.5 to protect critical system files or content	
2.1.23		Alerts if a piece of software is propagating across a given percentage of machines within a given timeframe	
2.1.24		Alerts if a piece of software is executed on a given percentage of machines within a given timeframe	
2.1.25		Alerts if a piece of software is blocked on a given percentage of machines within a given timeframe	
2.1.26		Alerts if a count for a piece of software surpasses a given threshold	
2.1.27		Alerts if, based on knowledgebase information, a piece of software is identified as being potentially harmful to the environment	
2.1.28		Ability to send syslog events in CEF to SIEM, as well as pivot	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
	from SIEM Console to endpoint based in hostname, IP Address for visibility into endpoint	
2.1.29	Complete two way integration and action to block network based malware on endpoints automatically	
2.1.30	Locate all systems with a given piece of software in real-time	
2.1.31	Save searches for monthly reporting needs	
2.1.32	Create and save baselines of standard desktops and laptops so that we can compare differences to production machines over time	
2.1.33	Create and save reports comparing individual computers against the baseline or groups of computers against the baseline	
2.1.34	Present graphs to visually represent drifting groups or computers	
2.1.35	Agent should be able to be installed remotely and silently with any of our software distribution tools	
2.1.36	End user should not be able to inspect, change, or delete any settings to the whitelist or blacklist	
2.1.37	Agent should protect itself from being stopped or removed, including the registry entries.	
2.1.38	The folder and files of the installed solution should be un-editable by users	
2.1.39	Manage end-user access to removable media (USB, CD-RW, external drives)	
2.1.40	Apply bans only for certain departments that should not have access to applications, or across the board for everyone	
2.1.41	Must be able to prevent banned software before first execution	
2.1.42	Automatically determine whether software is executable in nature regardless of file extension	
2.1.43	Ability to quickly move all systems, regardless of current policy, into lockdown	
2.2	**INCIDENT RESPONSE**	
2.2.1	Centralized storage of all endpoint event data	
2.2.2	Provides the ability to show which process, including version information and digital signature status, made a network connection	
2.2.3	Collect, at a minimum, the following events: process name/MD5, user context, file modification, registry modification, process	

ITEM		SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
		injections, network connections	
2.2.4		Collect endpoint data regardless of whether an event is deemed malicious or not (for example regardless of whether there is an IOC hit/match)	
2.2.5		Collect all endpoints events continuously and retains data for a minimum of 30 days	
2.2.6		Identify new and existing IOCs across the full enterprise in seconds	
2.2.7		CPU consumption on endpoint should be less than 1%, memory consumption should be less than 20MB	
2.2.8		The solution should provide process tree with clear indication of parent, child and sibling relationships	
2.2.9		Ability to view the events in a pictorial manner to easily identify all the related activities of the process in question	
2.2.10		Tagging of specific events such as registry changes, child process, module loads, network connections for further detailed analysis with relation to time of occurrence	
2.2.11		Automatically collect all executed binaries	
2.2.12		The agent based solution should be able to isolate the affected host remotely	
2.2.13		This agent based solution should able to remotely login to the system with the agent running and perform advance tasks	
2.2.14		Disrupt attacks through network isolation, process termination, process banning (aross all machines), delete files, etc	
2.2.15		All data and actions should be accessible via an easy to us and well published API (e.g., REST API).	
2.2.16		Should be able to integrate with various 'Threat Feeds' that provide indicators of comprise like blacklists of IP addresses, domains and MD5 sums out of the box without any additional licenses.	
2.2.17		Should be able to integrate with AV farms like VirusTotal for Malware detection	
2.2.18		Should be able to cross-reference with threat feeds from network vendors	
2.2.19		Ability to easily create threat feed for internally developed indicators of compromise	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
2.2.20	Ability to automatically search incoming event data for user-defined queries and alert on match	
2.2.21	Provide a secure forum and platform to share intelligence with the community	
2.2.22	Provides the ability to alert using syslog in a template manner for easy customization	
3.0	**PRIVILEGE ACCOUNT SECURITY**	
3.1	Solution should be a vaulting technology to automatically discovers and inventory privilege accounts throughout the IT environment.	
3.2	Has an option for Administrators to select which accounts or groups of accounts should be protected and automatically provision them to the Digital Vault	
3.3	Vault should include multiple built-in security layers to provide the strongest level of protection for privileged account information.	
3.4	Enforces granular access controls in accordance with organizational policy such as authorized users to access privileged accounts needed for day-to-day responsibilities.	
3.5	Should support automated workflows so that users may request access to accounts with elevated privileges as needed for legitimate business purposes	
3.6	The solution automatically rotates and synchronizes privileged account passwords in accordance with policy.	
3.7	Passwords can be automatically rotated after each use, at a regular cadence and on-demand.	
3.8	Vault should require users to "check-out" passwords before accessing privileged or shared accounts, and it can require users to provide specific justifications when requesting access to accounts with elevated privileges	
3.9	Automate threat containment by immediately invalidating potentially compromised privileged passwords.	
3.10	Has the capability to show auditors what privileged account policies and processes are in place, and easily report on which individual users accessed what, when and why	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
3.11	Must support the Multi Level Platform, Target System and OS: Windows Local/Domain Linux Solaris Databases Network Devices Via SSH and Telnet AS/400 (iSeries) zSeries (OS/390) Mainframe (Access Controll Software) Virtual Servers (eg. VMWare, Oracle VM, etc) Any SSH devices Supports Privilege Threat Analytics - Behavioural analysis Any ODBC devices	
3.12	Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism.	
3.13	Ability to integrate with LDAP/AD Directories.	
3.14	Ability to support querying and controlling access to passwords for nested global groups, including multiple forests, geographical locations, sophisticated LDAP searches and high performance queries.	
3.15	Ability to integrate with SIEM systems.	
3.16	Support Whitelisitng/blacklisting Unix commands	
3.17	Ability to integrate with ticketing systems.	
3.18	Ability to verify if a valid ticket exists and has the right status to retrieve a privileged password.	
3.19	Ability to automatically create a new trouble-ticket when retrieving a privileged password.	
3.20	Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)	
3.21	Ability to manage application embedded passwords	
3.22	Ability to support dual control - The system should support different configurations of approvals e.g. "4-eyes principle" when trying to retrieve a password including automatic email notification support.	
3.23	The proposed solution shall support user requesting the use of a target account for a future date/time.	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
3.24	Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phones.	
3.25	Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed)	
3.26	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.	
3.27	Supports a workflow approval process that only allows the direct manager of a requester to approve a request based on information from the LDAP server.	
3.28	Ability to support split password process where each half of a password can only be checked out by an authorized requester while storage of password is in full to ensure password is changed automatically.	
3.29	Ability to log workflow processes and/or have the ability to be reported or audited.	
3.30	The proposed solution shall provide UNIX users to use their preferred SSH clients while having their sessions recorded without logging in through the solution's preferred client.	
3.31	Ability to report on passwords that mismatch their policy	
3.32	Ability to report by system id or device type within a policy	
3.33	Ability to report on password status	
3.34	Reports should be customizable	
3.35	Audit data can be exported for use with, e.g. Crystal Reports	
3.36	Reports shall be automatically distributed by email	
3.37	Access to audit reports (and report configuration) shall be restricted to "auditor" end-users	
4.0	**SCOPE OF SERVICES & COMPETENCY REQUIREMENTS**	
4.1	**INSTALLATION AND START-UP**	
4.1.1	Hardware & Softare Start Up and Configuration Scope of Services	
4.1.2	Integration Scope of Services	
4.1.3	System Inter-Operability - Supplied equipment, devices and/or systems must not be proprietary and are capable of integration with a third (3rd) party open system monitoring platform	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
4.1.4	Work Plan/ Implementation Timeline in Gantt Chart with critical paths and dependencies reflected	
4.2	**TESTING AND COMMISSIONING**	
4.2.1	Preliminary Testing shall be based on Manufacturer approved training procedures. Provide high level description of the preliminary testing methodologies	
4.2.2	Perform Integrated Testing - provide high level description of the integrated testing methodologies	
4.2.3	Perform Penetration Tests - provide details on its methodologies, active data source and expected results summary	
4.3	**KNOWLEDGE TRANSFER**	
4.3.1	Equipment Technical Specifications briefing	
4.3.2	Appliance and Software Operations i.e. menu navigation, basic reconfiguration, and other relevant information pertaining to normal operations of the equipment	
4.3.3	Troubleshooting – provide sample occurrences and step by step procedures in addressing technical issues allowed by the equipment manufacturer to be carried out by the end-user without voiding active warranty	
4.3.4	Preventive Maintenance Orientation – conduct a detailed walk-through of the processes and/or procedures to be performed during Maintenance Services	
4.3.5	Include an On-the-Job (OJT) Training Program for DICT nominated staff. This program intends to skill up DICT personnel in the proper Operations and Maintenance of the installed equipment. The program should be facilitated by the winning vendor for 6 months from the date of issuance of Certificate of Final Acceptance	
4.4	**MAINTENANCE AND SUPPORT SERVICES**	
4.4.1	1-Year 24x7 unlimited email and phone support services	
4.4.2	1-Year Up to Level-2 Onsite Support with 4-hour response time within Metro Manila	
4.4.3	Support Service Structure – present the applicable Support Structure, Support Escalation Levels and valid contact details	

ITEM	SPECIFICATION	EXACT REFERENCE PAGE, SECTION AND/OR ITEM NO.
4.5	**VENDOR COMPETENCY COMPLIANCE**	
4.5.1	Technical Resources to be assigned to the project must possess valid certifications issued by the respective principals of the proposed solutions	
4.5.2	Manufacturer's Certificate/Distributor's Certificate certifying the bidder as skilled and authorized to resell, implement, operate, and maintain the proposed products and solutions	
4.5.3	Maintenance and Support Services to include Level 1 and 2 Technical Remote Support with 24 x 7 (phone or email) SLA	
4.5.4	Maintenance and Support Services to include Level 1 and 2 Technical On-site Support with 24 x 7 4-hour response time (within Metro Manila)	
4.5.5	Escalation procedures	
4.5.6	Technical Support Desk Facility	
4.6	**DOCUMENT ATTACHMENTS**	
4.6.1	Solution Diagrams	
4.6.2	Product Brochures of all proposed Equipment and/or Devices	
4.6.3	Professional CVs of engineering resources to be assigned.	
4.6.4	Technical Resources Certifications issued by relevant Principals	
4.6.5	Project Reference supporting documents	
4.6.6	Copies of Maintenance Agreements	

Name of Company	Signature Over Printed Name Of Authorized Representative	Date