Annex A

TECHNICAL PROPOSAL FOR THE BIDDING OF ANTIVIRUS AND ANTISPAM SOFTWARE WITH MAINTENANCE FOR THE PHILIPPINE DEPOSIT INSURANCE CORPORATION

NAME OF COMPANY : ______________________
ADDRESS : ______________________
TELEPHONE NO : ______________________
CONTACT PERSON : ______________________

FACT SHEET FOR ANTIVIRUS /ANTISPAM SOFTWARE WITH MAINTENANCE	MINIMUM MANDATORY REQUIREMENTS	PROPOSAL
1. Approved Budget for the Contract	[illegible] for three years	
2. Name of Antivirus / Antispam software	• Should be an internationally-recognized solution/trade name with presence and installation in major locations around the world specifically in Asia Pacific region	(please specify the proposed solutions/trade name)
3. General System Requirements	• Should provide user licenses for at least 1,200 workstations and 33 servers • Should provide user licenses for at least 700 Lotus Notes mailboxes/email users • Solution/System must run on Windows Operating System and supports Windows 2000SP4 or higher versions on a server with the following minimum hardware specification: • 2 Intel Xeon 2.4 GHz • 200GB Hard Disk • 2 GB Memory • Should have at least two (2) operational installations in the Philippines with at least 1,000 user licenses.	
4. Scanning Module for Workstations and Servers	• Monitors all virus entry points, including disks, programs, documents, network drives, CD-ROM, email and Internet downloads at the desktop. • Minimum bandwidth usage during scanning of servers and workstations • Can automatically repair virus registry entries, delete virus in memory and repair system files modified by virus i.e. win.ini • Performs kernel-level scanning for viruses and malicious code via Microsoft to minimize performance degradation. Uses a multi-threaded scan engine to enhance the speed of scanning files and minimize the impact to the server. • Automatically removes malware from local and remote clients • Identifies infected clients by specific IP address and machine name with detailed reporting to support comprehensive cleanup • Blocks virus carriers and prevents viruses from propagating and jamming networks through the use of policies. • Allows administrators to deliver outbreak prevention policies that provide early warning to prevent or contain outbreaks before patches, pattern files, or network signatures are deployed. • Provides management of multiple workstations and servers from a web-based console that enables administrators to deploy programs and updates to workstations and servers simultaneously, and monitor status in real time, including pattern file and program versions, infection status, and connection status for all workstations and servers.	

FACT SHEET FOR ANTIVIRUS /ANTISPAM SOFTWARE WITH MAINTENANCE	MINIMUM MANDATORY REQUIREMENTS	PROPOSAL
	• Requires no end-user intervention during installation and update. • Cannot be disabled or uninstalled by end ordinary users. • Configured to download virus pattern files and scan engine updates automatically and then distribute them to designated workstations and servers. • Uses an incremental update mechanism so that the designated servers only download the new virus pattern files that have been added since the last version, which saves download time and preserves network bandwidth. • Provides comprehensive reporting facility including customizable and printable reports • Capable of presenting detailed reports i.e. number of workstations affected per day; number of viruses captured; action taken • Presentation of reports in graphical format • Should be compatible with workstations and servers running on Windows XP and higher versions with the following minimum hardware specifications: • Pentium IV 2 Ghz, 40GB HD, 512 MB Memory	
5. Scanning Module for Two (2) Lotus Domino Servers	• Scans content of inbound and outbound email to help prevent the loss of confidential or proprietary information and trade secrets and exposure to legal liability. • Detects attachments by file name, true file type, file extension, and attachment content-type. • Detects viruses in compressed attachments, including recursive archives • Blocks non-business related files or oversized attachments from entering the system, increasing network performance. • Supports multiple email usage policies, enabling administrators to define scanning and notification rules for both inbound and outbound traffic i.e. rules on file size attachment, rule on the type of attachment, etc. • Enables outbreak prevention services to provide a proactive response to new virus threats, helping ensure that inbound email does not contain malicious code embedded in SMTP traffic. • Helps avert potential threats by removing suspicious attachment file types before the virus pattern is available. • Protects against malware (viruses, worms, Trojans, and other malicious code) by blocking the attachment types used by viruses, and it scans all email with embedded JavaScript or ActiveX code. • Provides management of server from a Lotus Domino administrator program. The management monitors status in real time, including pattern file and program versions and infection status. • Configured to download virus pattern files and scan engine updates automatically. • Uses an incremental update mechanism so that the designated servers only download the new virus pattern files that have been added since the last version, which saves download time and preserves network bandwidth.	

FACT SHEET FOR ANTIVIRUS /ANTISPAM SOFTWARE WITH MAINTENANCE	MINIMUM MANDATORY REQUIREMENTS	PROPOSAL
6. SMTP Gateway Software including Scanning Module	• Detects and disinfects virus at the mail gateway • Gateway security triggers automatic cleanup on clients • Enforce regulatory compliance, coordinated defense against email threats and prevent data leakage through its intuitive policy settings. Filters inbound and outbound email and attachments based on keywords, lexicons, attachment characteristics, and other content security rules. For more customized content filtering, users can construct rules using Boolean and regular expressions. • Filtering the mail by attachment file type such as, but not limited to the following: • potential virus infected (*.exe, *.com, *.dll, *.drv, *.bin, *.ovl, *.sys) • audio files (*.wav, *.mp3, midi) • video files (mpeg, msvideo format, quicktime format) • Blocks IP addresses of known phishers, signatures of phishing emails, and heuristics specifically aimed at phishing emails to provide an effective, combined approach against phishing emails thereby improving protection against identity theft and loss of confidential information of both corporate data and employee personal information. • Compliments with the web scanning module to block transmission of outbound data to known phishing-related Web sites. • Identifies computers by their Internet address and adds them to the blacklist that is checked in real time by the e-mail server. An email sent from a blacklisted server will be refused. • Notifies admin and or sender/recipient that the message was unacceptable • Create rules to automatically delete or process blocked email such as sending to junk or quarantine box • Allows administrators to create/configure simple and easy ruleset • Allows administrator to designate authorized senders and recipients by company, group, or individual and can set the appropriate enforcement action for each policy. • Allows administrator to add company-specific legal disclaimers to outgoing email based on message content characteristics. • Compatible with Microsoft Windows and Linux and allows for flexible configurations with multiple servers while a single Web-based management console enables administrator to monitor status in real time, including pattern file and program versions, policy, configurations, logging and reporting. • Configured to download virus pattern files and scan engine updates automatically. • Uses an incremental update mechanism so that the designated servers only download the new virus pattern files that have been added since the last version, which saves download time and preserves network bandwidth.	

FACT SHEET FOR ANTIVIRUS /ANTISPAM SOFTWARE WITH MAINTENANCE	MINIMUM MANDATORY REQUIREMENTS	PROPOSAL
7. Internet Proxy Server with Scanning Module for Web	• Protects the local area network against Web-based attacks, including viruses, Trojans, worms, spyware, grayware and phishing. • Enables administrators to manage employee Internet use by limiting access by category, group or user, time of day, day of week, and bandwidth quotas. • Filters Web content through its database where URLs are categorized to effectively identify and block inappropriate Web sites. • Blocks websites based on specified categories such as, but no limited to sexual explicit / graphic materials, gambling, gaming and other sites that pose security threats and similar contents • Provides management of servers from a web-based console. The console enables administrators to monitor status in real time, including pattern file and program versions, policy, configurations, logging and reporting. • Configured to download virus pattern files and scan engine updates automatically. • Uses an incremental update mechanism so that the designated servers only download the new virus pattern files that have been added since the last version, which saves download time and preserves network bandwidth.	
8. Maintenance/ Product Upgrade, Update and Technical Support	• Should provide 24 x 7 technical support, with unlimited telephone support • Free software updates and upgrades for the duration of the maintenance agreement, which shall be at least three (3) years.	
9. Deployment	• Must be able to show all the required modules/features specified in the Factsheet within 5 working days after being declared as the Lowest Calculated Bidder (LCB) through a Proof of Concept or actual site visit to an operational site as a pre-requisite for post-qualification. • Must be deployed/installed by the winning bidder in all PDIC servers/workstations within 30 working days after the contract was signed by both parties. • Should submit a detailed work plan outlining the timetable of activities during deployment and implementation and identifying the responsibilities of the entities who will be involved in the project • Provide whatever is necessary to ensure that the system/solution will be properly installed and working as specified in the Factsheet. • Must provide the necessary system documentations which include but not limited to User Manual, System Administration Manual, etc.	
10. Trainings	• At least two (2) technical trainings for the Administrators of the proposed solution. • At least two (2) Network and/or System Security Trainings for the Administrators of the proposed solution.	

NAME OF AUTHORIZED REPRESENTATIVE OF BIDDER : ____________________
POSITION : ____________________
SIGNATURE : ____________________
DATE OF OPENING OF BIDS : ____________________