Jakarta, 02 FEB 2017

Nomor : PFA/3.2/ 563

PENGUMUMAN LELANG

Dengan ini diumumkan bahwa BNI - Divisi Pengelolaan Aset dan Pengadaan akan melaksanakan Pelelangan Terbatas di antara Rekanan Terdaftar BNI sebagai berikut :

1. **Lingkup Pekerjaan**

Paket Pekerjaan	: Pengadaan Barang dan Jasa
Tujuan Proyek	: **Pengadaan Perangkat Advanced Anti Malware Internet Security System**
Ruang Lingkup	: Pengadaan 2 (dua) unit perangkat security *Web Application Firewall* yang dibutuhkan dan jasa implementasi sesuai kebutuhan BNI.
Alamat Proyek	: PT Bank Negara Indonesia (Persero) Tbk Divisi Operasional Teknologi Informasi Jl. Jend. Sudirman Kav. 1 – Jakarta

2. **Syarat Peserta Pelelangan :**
   a. Memiliki Tanda Daftar Rekanan (TDR) BNI yang sampai saat ini masih berlaku dibuktikan dengan Copy TDR, atau apabila dalam proses perpanjangan maka dibuktikan dengan Surat Keterangan Perpanjangan TDR dalam Proses dari BNI.
   b. Peserta terdaftar sebagai rekanan di Bank BNI dengan kondisi sebagai berikut :
      - Bidang Usaha : **Jasa Pemasok Barang dan Jasa Lainnya.**
      - Sub Bidang Usaha & Kualifikasi :
        i. Jasa Teknologi dan Sistem Informasi, kualifikasi : minimal **M.**
        ii. Teknologi Informasi, kualifikasi : minimal **M.**
        iii. Alat/Peralatan/Suku Cadang : komputer , kualifikasi : minimal **M.**
   c. Merupakan Nasabah BNI dan memiliki Referensi Bank dari BNI.
   d. Peserta adalah perusahaan yang menyediakan barang dan/atau jasa dimaksud dan telah menjadi rekanan BNI.
   e. Peserta mendapat dukungan dari Principal atas perangkat yang ditawarkan yang dibuktikan dengan surat dukungan dari Principal atas produk yang ditawarkan.
   f. Surat pernyataan bermaterai, yang menerangkan bahwa perusahaan tersebut tidak dinyatakan pailit melalui keputusan pengadilan, usahanya tidak sedang dihentikan sementara, dan orang yang mewakili badan usaha tersebut tidak sedang menjalani sanksi pidana.
   g. Peserta memiliki helpdesk support.
   h. Principle/Distributor/peserta telah mempunyai pengalaman mengelola atau mengimplementasikan produk security yang ditawarkan tersebut diperusahaan finansial / banking /provider di Indonesia dengan proyek sejenis (referensi pekerjaan sejenis yang dibuktikan oleh copy Surat Perintah Kerja/Kontrak/Purchase Order/Delivery Order/Sales Order dari salah satu client).
   i. Sanggup memenuhi terms and conditions.
   j. Sanggup memenuhi ruang lingkup pengadaan.

PT. Bank Negara Indonesia (Persero) Tbk
Kantor Besar
Jl. Jenderal Sudirman Kav. 1
Jakarta 10220, Indonesia
www.bni.co.id

3. **Pendaftaran Peserta Lelang :**
Bagi Rekanan Terdaftar BNI yang berminat mengikuti pelelangan tersebut dapat mendaftarkan diri dengan memasukkan *Surat Pendaftaran Peserta Pelelangan (Hardcopy)* dan S*oftcopy* (**CD dengan diberikan <u>label perusahaan dan nama proyek</u>**) dengan melampirkan :

a. Surat pengantar mengikuti lelang.
b. Copy surat telah tercatat sebagai rekanan BNI (TDR), atau apabila dalam proses perpanjangan maka dibuktikan dengan Surat Keterangan Perpanjangan TDR dalam Proses dari BNI.
c. Asli Referensi Bank dari BNI.
d. Daftar Pengurus Perusahaan (Direksi, Komisaris dan Pemegang Saham), sesuai dengan akte perusahaan.
e. Surat Pernyataan yang ditandatangani oleh Direktur atau Pejabat yang berwenang dan bermaterai boleh dibuat terpisah atau digabung, yang menyatakan bahwa :
   e.1. Surat kesanggupan untuk memenuhi ruang lingkup pengadaan.
   e.2. Surat pernyataan bahwa spesifikasi yang ditawarkan telah sesuai dengan spesifikasi yang diminta oleh BNI dan tidak akan ada penurunan spesifikasi teknis saat delivery barang.
   e.3. Surat kesanggupan untuk memberikan maintenance, support dan garansi perangkat yang ditawarkan (hardware dan software termasuk lisensi).
   e.4. Surat pernyataan bersedia memberikan After Sales Support.
   e.5. Surat dukungan dari Principal atas barang yang ditawarkan, harus disebutkan dengan jelas detail spesifikasi barang
   e.6. Surat kesanggupan untuk memenuhi Terms and Conditions
   e.7. Surat kesanggupan untuk melakukan delivery barang tepat pada waktunya, dan apabila terlambat bersedia dikenakan sanksi.
   e.8 Surat pernyataan bahwa resources (enginer/teknisi/expertise) yang ditugaskan dalam proyek ini sesuai dengan yang disampaikan dalam proposal yang diserahkan kepada BNI.

4. Rekanan BNI yang berminat mendaftar lelang harus menyampaikan seluruh persyaratan pendaftaran lelang secara lengkap serta melampirkan bukti penyetoran pendaftaran lelang sebesar **Rp 250.000,-** (dua ratus lima puluh ribu rupiah) ke rekening BNI Divisi Procurement And Fixed Asset ***"Pendapatan Non Operasional"*** Nomor Rekening : **723.360.490859.001.**

5. **Alamat pendaftaran :**

PT. Bank Negara Indonesia (Persero) Tbk
Divisi Pengelolaan Aset dan Pengadaan
Gedung BNI Lt. 5
CBD BSD City Lot I/5
Jl. Pahlawan Seribu - Tangerang Selatan

Pendaftaran dimulai dari tanggal 03 FEB 2017 s/d tanggal 08 FEB 2017

Contact Person : Hilman Akbar (hilman.akbar@bni.co.id)

Bagi para pendaftar yang tidak memenuhi persyaratan sebagaimana butir (2) dan (3) di atas dinyatakan gugur dan calon peserta lelang yang memenuhi syarat akan diumumkan selanjutnya.

Demikianlah pengumuman ini untuk diketahui oleh Rekanan Terdaftar BNI.

PT Bank Negara Indonesia (Persero) Tbk
Panitia Pelelangan

PT BANK NEGARA INDONESIA (PERSERO) Tbk * KANTOR PUSAT *

Wahyu Purwandaka
Wakil Pemimpin

Spesifikasi Teknis

Minimum requirement Mandatory :

Advanced anti malware untuk network
Memiliki solusi unknown malware / Advanced Threat Protection/advanced anti malware dengan kapasitas Throughput network sebesar 3 Gbps yang mensupport 4X 10 Gbps dan 3 x 1 Gbps interface network environment dengan fitur sebagai berikut : - Dapat melakukan deteksi terhadap file EXE, PDF, Flash, RTF, dan lain-lain - Dapat melakukan deteksi dan analisa terhadap tahap-tahap yang umum ditemui pada serangan berbasis APT seperti: Information Gathering, Point of Entry, CnC Communication, Lateral Movement, Asset Discovery, Data Exfiltration - Dapat melakukan analisa terhadap aktifitas network dari ancaman yang terdeteksi (tipe malware, severity, sumber, atau target komunikasi) - Mendeteksi komunikasi dengan kategori Command and Control (CnC) yang mungkin diinisiasi oleh malicious agent (bot) di dalam jaringan internal - Memiliki kemampuan sandboxing dengan multiple built-in virtual execution environment untuk mensimulasi aktifitas file dan mendeteksi perilaku yang diduga mencurigakan - Mendukung minimal 3 OS yang dapat dimasukkan dalam sandbox, diantaranya Win XP ,win 7, win 8, win 10, win server 2008 , win server 2012 dan versi diatasnya. - Minimal memiliki virtual execution environment sandbox masing masing OS sebanyak 5 secara simultant untuk mempercepat *inspection file* - Solusi dapat menganalisa file berukuran lebih dari 10 MB - Dapat melakukan deteksi dan analisa terhadap tahap-tahap yang umum ditemui pada serangan berbasis APT (advanced persistent threat) /ATP(advandced threat protection) seperti: Information Gathering, Point of Entry, CnC Communication, Lateral Movement, Asset Discovery, Data Exfiltration
Dapat mendeteksi serangan Zero Days oleh metode anomaly protokol dan aplikasi

Advanced anti malware untuk email
Advanced anti malware untuk email sistem BNI existing dengan kapasitas 300.000 email/hari dan concurrent user 1.500
Memiliki fitur yang dapat mensimulasikan phising URL link yang ada di dalam pesan email dengan interface mendukung 1 Gbps copper.
Memiliki solusi unknown malware / Advanced Threat Protection/advanced anti malware untuk email system BNI existing yang mensupport 2 X 1 Gbps Interface dengan fitur sebagai berikut: - Dapat mensimulasikan file di dalam email yang mengandung unknown malware dengan system virtual Sandbox dapat mendeteksi dan melakukan pencegahan

ketika ada perilaku yang mencurigakan seperti:

- Exploit code
- Koneksi ke tujuan di Internet dengan kategori berbahaya
- Koneksi ke Command and Control server
- Melakukan self-replication
- Melakukan infeksi ke file-file lain
- Melakukan download atau drop executable file lain
- Memodifikasi startup process atau program critical lain
- Membuka port-port yang tidak umum
- Melakukan self-delete
- Mendeteksi lingkungan virtual
- Melakukan sleep
- Dan lainnya

- Mendeteksi dan menganalisa URL di email body , subjek email, dan yang disertakan dalam file attachment MS Office dan PDF
- Mendukung metode scanning berbasis reputasi dan juga secara heuristic
- Melakukan deteksi terhadap unsigned executable file
- Mendeteksi, mendownload dan menganalisa file yang disertakan di email message body
- Menyediakan fasilitas karantina untuk suspicious email yang match dengan kriteria tertentu