Instytut Badań Systemowych Polskiej Akademii Nauk

ul. Newelska 6, 01-447 Warszawa

Centrala: (0) 22 381 01 00
Dyrekcja: (0) 22 381 02 75
Fax: (0) 22 381 01 05
E-mail: ibs@ibspan.waw.pl
Web: www.ibspan.waw.pl
NIP: 525 000 86 08

Warszawa 8 lipca 2010 r.

Nr sprawy: F1-208-07/10

Instytut Badań Systemowych PAN informuje o wszczęciu postępowania prowadzonego w trybie przetargu nieograniczonego poniżej 5278000 Euro na:

Dostawę urządzeń komputerowych do IBS PAN

1. **Nazwa oraz adres Zamawiającego**
   Instytut Badań Systemowych PAN ; 01-447 Warszawa ul. Newelska 6.
   REGON 000686434
   NIP 525-000-86-08

Tryb udzielenia zamówienia
Postępowanie o udzielenie zamówienia publicznego prowadzone jest w oparciu o przepisy ustawy z dnia 29 stycznia 2004 - Prawo zamówień publicznych (Dz.U. z 2007 r. Nr 223, poz. 1655, z 2008 r. Nr 171, poz. 1058, Nr 220, poz. 1420 i Nr 227,poz. 1505 oraz z 2009 r. Nr 19, poz. 101, Nr 65, poz. 545, Nr 91, poz. 742, Nr 157, poz.1241, Nr 206, poz. 1591, Nr 219, poz. 1706 i Nr 223, poz. 1778) w trybie przetargu nieograniczonego.

2. **Opis przedmiotu zamówienia**
   Przedmiot zamówienia obejmuje:

   1. System zabezpieczenia sieciowego (Firewall sprzętowy) typu A – 1 sztuka
   2. Przełączniki sieciowe typu B – od 2 do 5 sztuk
   3. Serwer typu C – 1 sztuka

Ad. 1

1. System zabezpieczenia sieciowego

Właściwości wielozadaniowego systemu zabezpieczeń sieciowych:

1. System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułów: zarządzania, modułu wykonującego operacje kryptograficzne, modułu analizy ruchu w warstwie aplikacyjnej oraz modułu odpowiedzialnego za operacje sieciowe (ruting, translacje NAT, ARP lookup). Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
3. Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż 500 Mb/s dla kontroli firewall, nie mniej niż 500 Mb/s dla inspekcji ruchu w warstwie aplikacyjnej i obsługiwać nie mniej niż 250 000 jednoczesnych połączeń.

4. Urządzenie zabezpieczeń musi być wyposażone w co najmniej 12 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 4 interfejsów optycznych (SFP).
5. System zabezpieczeń musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym (tzn. w warstwie 2 modelu OSI) oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych. Musi istnieć możliwość jednoczesnej konfiguracji poszczególnych interfejsów w różnych trybach.
6. Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać nie mniej niż 3 wirtualne rutery posiadających odrębne tabele rutingu. Urządzenie musi obsługiwać protokoły Turingu dynamicznego, nie mniej niż RIP i OSPF.
7. System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
8. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa.
9. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (oznaczenia DiffServ).
10. System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit, wirus, złośliwy kod.
11. System zabezpieczeń musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
12. System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
13. System zabezpieczeń musi identyfikować co najmniej 700 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS nie mniej niż: Skype, Gada-Gadu, Tor, BitTorrent, eMule. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall.
14. System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN).
15. System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ.

16. System zabezpieczeń musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, encrypted ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
17. System zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS) bez konieczności dokupywania jakichkolwiek komponentów, jeśli funkcja taka objęta jest subskrypcją to subskrypcją ta powinna być uwzględniona w ofercie.
18. System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej, kontrolującego przynajmniej pocztę elektronicznej (SMTP, POP3, IMAP), FTP oraz http bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza AV musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny.
19. Baza AV musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny.
20. System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupywania jakichkolwiek komponentów, poza subskrypcją. Baza WF musi być przechowywania na urządzeniu i regularnie aktualizowana w sposób automatyczny.
21. System zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z Active Directory i serwerami terminali). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości ma odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
22. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI), graficznej konsoli Web GUI oraz scentralizowanego systemu zarządzania. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
23. System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
24. System zabezpieczeń zapewnia możliwość bezpiecznego zdalnego dostępu do chronionych zasobów w oparciu o standard SSL VPN bez konieczności stosowania dodatkowych licencji.
25. System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
26. Wraz z urządzeniem powinna zostać dostarczona drugie identyczne pod względem parametrów sprzętowo-programowych urządzenie „spare” pozbawione licencji i przeznaczone do wymiany w przypadku uszkodzenia jednostki podstawowej.

27. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.
28. Sprzęt nowy wraz z 5 letnią gwarancją. Wymagane wdrożenie w sieci komputerowej IBS PAN oraz przeszkolenie pracowników Ośrodka Komputerowego IBS PAN. Przykładowe urządzenie spełniające warunki to PALO ALTO Networks - 2050 w wersji On-Site Spare.

W ramach postępowania musi zostać dostarczone jedno kompletne, gotowe do pracy urządzenie. Wraz z produktem wymagane jest dostarczenie opieki technicznej ważnej przez okres 5 lat. Opieka musi zawierać:

- wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela,
- wymianę uszkodzonego sprzętu,
- dostęp do nowych wersji oprogramowania,
- aktualizację bazy ataków IPS i definicji wirusów, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

Ad. 2
Przełączniki sieciowe typu B

- Wewnętrzne porty wejścia/wyjścia co najmniej 44 porty 10/100/1000 z automatycznym wykrywaniem szybkości (10Base-T typu IEEE 802.3, 100Base-TX typu IEEE 802.3u, 1000Base-T typu IEEE 802.3ab); Tryb dupleks: 10Base-T/100Base-TX: pełny dupleks lub półdupleks; 1000Base-T: tylko pełny dupleks; Typy nośników: Auto-MDIX; co najmniej 4 porty typu dual personality — każdy może służyć jako port RJ-45 10/100/1000 (10Base-T typu IEEE 802.3; 100Base-TX typu IEEE 802.3u; 1000Base-T Gigabit Ethernet typu 802.3ab) lub jako gniazdo mini-GBIC (na transceivery mini-GBIC).
- Przepustowość maks. co najmniej 131 mln p/s
- funkcja rutingu/przełączania co najmniej 176 Gb/s
- obsługiwane standarty co najmniej Komunikacja RFC 1591 DNS (klient); zarządzanie przez WWW (HTML) i telnet; IEEE 802.1D MAC Bridges; Priorytet IEEE 802.1p; Sieci VLAN IEEE 802.1Q; IEEE 802.1s Multiple Spanning Trees; Klasyfikacja sieci VLAN w standardzie IEEE 802.1v według protokołów i portów; IEEE 802.1w Rapid Reconfiguration of Spanning Tree; IEEE 802.3ad Link Aggregation Control Protocol (LACP); IEEE 802.3x Flow Control; RFC 768 UDP; Protokół RFC 783 TFTP (wersja 2); RFC 792 ICMP; RFC 793 TCP; RFC 826 ARP; RFC 854 TELNET; RFC 868 Time Protocol; RFC 951 BOOTP; RFC 1058 RIPv1; Protokół RFC 1350 TFTP (wersja 2); RFC 2030 Simple Network Time Protocol (SNTP) v4; RFC 2131 DHCP; RFC 2453 RIPv2; RFC 3046 DHCP Relay Agent Information Option; RFC 3376 IGMPv3 (tylko dołączanie hosta); RFC 1981 IPv6 Path MTU Discovery; RFC 2460 IPv6 Specification; RFC 2710 Multicast Listener Discovery (MLD) for IPv6; RFC 2925 Remote Operations MIB (tylko pingowanie); RFC 3019 MLDv1 MIB; RFC 3315 DHCPv6 (tylko klient); RFC 3513 IPv6 Addressing Architecture; RFC 3596 DNS Extension for IPv6; RFC 3810 MLDv2 (tylko dołączanie hosta); RFC 4022 MIB for TCP; RFC 4113 MIB for UDP; RFC 4251 SSHv6 Architecture; RFC 4252 SSHv6 Authentication; RFC 4253 SSHv6 Transport Layer; RFC 4254 SSHv6 Connection; RFC 4293 MIB for IP; RFC 4419 Key Exchange for SSH; RFC 4443 ICMPv6; RFC 4541 IGMP & MLD Snooping Switch; RFC 4861 IPv6 Neighbor Discovery; RFC 4862 IPv6 Stateless Address Auto-configuration; RFC 1213 MIB II; RFC 1493 Bridge MIB; RFC 1724 RIPv2 MIB; RFC 2021 RMONv2 MIB; RFC 2613 SMON MIB; RFC 2618 RADIUS Client MIB; RFC 2620 RADIUS Accounting MIB; RFC 2665 Ethernet-Like-MIB; RFC 2668 802.3 MAU MIB; RFC 2674 802.1p i IEEE 802.1Q Bridge MIB; RFC 2737 Entity MIB (wersja 2); RFC 2863 The

Interfaces Group MIB; RFC 2474 DiffServ Precedence, 8 kolejek na port; RFC 2597 DiffServ Assured Forwarding (AF); RFC 2598 DiffServ Expedited Forwarding (EF) Ingress Rate Limiting; IEEE 802.1X Port Based Network Access Control RFC 1492 TACACS+; RFC 2138 RADIUS Authentication; RFC 2866 RADIUS Accounting; Protokół Secure Sockets Layer (SSL).

- Rozmiar Tabeli Adresów co najmniej 2000 pozycji
- Montaż na stojaku 19”
- Stan utajenia 1000 Mb: < 2,9 µs (64-bajtowe pakiety FIFO); 10 Gb/s: < 1,3 µs (64-bajtowe pakiety FIFO).
- Zasilanie zewnętrzne 100–127 V / 200–240 V; 50/60 Hz
- Pobór mocy co najwyżej 105 W
- Dostępność zasilania 2,1 A/ 1,1 A
- Firmware (updaty) bezpłatnie dostępne od producenta przez cały okres życia produktu
- Sprzęt fabrycznie nowy gwarancja life time przykładowy sprzęt spełniający warunki to: HP ProCurve 2910al-48G (J9147A)

Ad. 3

Serwer typu C

- obudowa mająca zasilacz nie gorszy niż oraz dysponująca ilością miejsca na dyski nie mniejszym niż CSE-846TQ-R1200B Supermicro Chassis CSE-846TQ-R1200B, 4U, SATA/SAS (SES2), Redundant PSU 1200W, Black
- napęd DVD
- 2 sztuki SNK-P0034AP4 4U+, Active CPU Heatsink, SC743's w/ X7 DP Workstation
- Płyta główna obsługująca procesory oraz posiadająca złącza w ilości nie mniejszej niż MBD-X8DTI-LN4F-O Supermicro MBD-X8DTI-LN4F-O, Dual Processor, Intel 5520 (Tylersburg) Chipset, SATA, 4x LAN, IPMI, Motherboard - Retail
- Kontroler SATA obsługujący 24 kanały SATA + obsługujący standarty RAID oraz posiadający funkcjonalność nie gorszą niż 9650SE-24M8 KIT 3ware 9650SE-24M8 Internal SATA II Hardware RAID Controller Card, Kit
- Bateria podtrzymująca opóźniony zapis na dysk o parametrach nie gorszych niż BBU-MODULE-03 Battery Backup Unit for 3ware 9650SE/9590SE/9550SX(U) HW RAID Controllers
- 2 sztuki **zestawów** pamięci o parametrach timingowych (oraz szybkości taktowania) nie gorszych niż KVR1333D3S4R9SK3/6G 6GB 1333MHz DDR3 ECC Reg CL9 DIMM (Kit of 3) SR x4 w/TS
- 2 sztuki procesorów o parametrach nie gorszych niż (ilość jąder, szybkość taktowania, ilość pamięci cache) BX80602E5506 E5506 Xeon processor (quad core) *** 2.13 4M 4.80 GT/sec
- 24 sztuki dysków o pojemności, ilości pamięci cache, gwarancji, MTBF, szybkości transferu, szybkości naprawy błędów TLAR nie gorszej niż WD2002FYPS HDD Desktop WESTERN DIGITAL RE4-GP 2000GB 7200rpm, Native Command Queuing (NCQ) 64MB cache Serial ATA II-300
- Sprzęt fabrycznie nowy gwarancja co najmniej 36 miesięcy

3. **Termin wykonania zamówienia**
   Wykonawca zrealizuje zamówienie do dnia 15 września 2010 r.

4. **Wadium**: oferta musi być zabezpieczona wadium w następującej wysokości 2000 zł (część pierwsza) lub/i 1000 zł (część druga) lub/i 1000 zł (część trzecia), wadium może być wniesione w formie:

   1. pieniądza,

   2. poręczenia bankowego lub poręczenia spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym,

   3. gwarancji bankowych

   4. gwarancji ubezpieczeniowych,

   5. poręczenia przez podmioty, o których mowa w art.6b ust.5 pkt 2 ustawy z dnia 9 listopada 2000r o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz.U.Nr 109, poz. 1158, z późn.zm.).

   Wadium w formie pieniądza należy wnieść najpóźniej do dnia składania ofert na konto 53 1240 5918 1111 0000 4913 5291

   Wadium wnoszone w formie poręczeń, gwarancji bankowej lub ubezpieczeniowej należy złożyć w formie oryginału wraz z ofertą.

   Wadium musi być wniesione najpóźniej w terminie składania ofert tj. do dnia 15.09.2010 r.

   Zamawiający jest zobowiązany niezwłocznie zwrócić wadium, jeżeli:

   a) upłynął termin związania z ofertą,

   b) zawarto umowę w sprawie zamówienia publicznego i wniesiono zabezpieczenie należytego wykonania umowy,

   c) zamawiający unieważnił postępowanie, a protesty zostały ostatecznie rozstrzygnięte lub upłynął termin ich składania,

   d) na pisemny wniosek Wykonawcy, który wycofał ofertę przed terminem składania ofert, który został wykluczony, którego oferta została odrzucona.

5. **Opis warunków udziału w postępowaniu oraz opis sposobu dokonywania oceny spełniania tych warunków. Dotyczy wszystkich części.**
   O zamówienie mogą się ubiegać wykonawcy, którzy spełniają warunki określone w art. 22 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień, a w szczególności:

   1) posiadają uprawnienia do wykonywania działalności lub czynności określonej przedmiotem zamówienia, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień,

   2) posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia,

   3) znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia,

   4) nie podlegają wykluczeniu z postępowania o udzielenie zamówienia,

   Oceny spełnienia warunków Zamawiający dokona na podstawie złożonych przez wykonawcę oświadczeń oraz dokumentów wskazanych w pkt. 8 niniejszej SIWZ.
   Zgodnie z art. 23 ustawy wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takiej sytuacji, wymagane jest ustanowienie pełnomocnika do reprezentowania w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
   Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia.
   Ocena spełnienia warunków wymaganych od wykonawców zostanie dokonana wg formuły „spełnia-nie spełnia". Niespełnienie któregokolwiek warunku spowoduje wykluczenie wykonawcy z postępowania i uznanie jego oferty za odrzuconą.

6. Oceny spełnienia warunków Zamawiający dokona na podstawie złożonych przez wykonawcę oświadczeń oraz dokumentów wskazanych w pkt 6 i 8 niniejszej SIWZ. Zgodnie z art. 23 ustawy wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia. W takiej sytuacji, wymagane jest ustanowienie pełnomocnika

do reprezentowania w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Przepisy dotyczące wykonawcy stosuje się odpowiednio do wykonawców wspólnie ubiegających się o udzielenie zamówienia. Ocena spełnienia warunków wymaganych od wykonawców zostanie dokonana wg formuły "spełnia / nie spełnia". Niespełnienie któregokolwiek warunku spowoduje wykluczenie wykonawcy z postępowania i uznanie jego oferty za odrzuconą.

7. **Wykaz oświadczeń i dokumentów, jakie mają dostarczyć wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu**
   W celu potwierdzenia spełniania warunków udziału w postępowaniu oraz w celu umożliwienia dokonania oceny oferta musi zawierać następujące dokumenty (dokumenty są składane w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez wykonawcę w następującej kolejności):

Lp	**Warunki wymagane od Wykonawcy ubiegającego się o zamówienie**	**Dokumenty potwierdzające spełnienie wymaganych warunków**
1	Oferta	Wypełniony Formularz Ofertowy - Załącznik nr 1
2	Nie podleganie wykluczeniu z postępowania o udzielenie zamówienia	Oświadczenie, że Wykonawca spełnia warunki udziału w postępowaniu, określone w art.22 – Załącznik nr 2
3	Potwierdzenie wniesienia Wadium	Dowody wpłat wadium (kopie) lub poręczeń bankowych, gwarancji bankowych, gwarancji ubezpieczeniowych

8. **Informacja o sposobie porozumiewania się Zamawiającego z wykonawcami**
   Oświadczenia, wnioski, zawiadomienia oraz informacje przekazywane są pisemnie, faksem lub drogą elektroniczną. Jeżeli zamawiający lub wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub drogą elektroniczną, każda ze stron, na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania. Osobami uprawnionymi przez Zamawiającego do kontaktu z wykonawcami są:

   Instytut Badań Systemowych Polskiej Akademii Nauk,
   Bartłomiej Solarz-Niesłuchowski,
   Newelska 6, 01-447 Warszawa, woj. mazowieckie,
   tel. 223810247,
   fax 223810105, e-mail: Bartłomiej.Solarz@ibspan.waw.pl

   Instytut Badań Systemowych Polskiej Akademii Nauk,
   Krzysztof Szkatuła,
   Newelska 6, 01-447 Warszawa, woj. mazowieckie,
   tel. 223810130,
   fax 223810210, e-mail: Krzysztof.Szkatula@ibspan.waw.pl

   Godziny pracy Zamawiającego: od poniedziałku do piątku w godz. od 8.00 do 16.00.

9. **Termin związania ofertą**
   Termin związania ofertą wynosi 30 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

10. **Opis sposobu przygotowywania ofert**

- Wykonawca może złożyć tylko jedną ofertę.
- Wszelkie zmiany w ofercie powinny być parafowane przez wykonawcę.
- Koszty związane z przygotowaniem i dostarczeniem oferty ponosi wykonawca.
- Oferta musi być podpisana przez osobę (osoby) upoważnioną do reprezentowania wykonawcy na zewnątrz.
- W przypadku, gdy wykonawcę reprezentuje inna osoba aniżeli wskazana w treści aktualnego odpisu z właściwego rejestru lub zaświadczenia o wpisie do ewidencji (w szczególności pełnomocnik inny niż prokurent) do oferty należy załączyć dokument potwierdzający umocowanie tej osoby do złożenia oferty - w oryginale lub notarialnie poświadczonej kopii (np. dokument pełnomocnictwa).
- Pełnomocnictwo powinno jednoznacznie określać zakres umocowania i wskazywać osobę pełnomocnika; w przypadku podmiotów występujących wspólnie w dokumencie

pełnomocnictwa należy wskazać wszystkich wykonawców, którzy wspólnie ubiegają się udzielenie zamówienia, a każdy z nich powinien podpisać się pod tym dokumentem.

- Treść oferty musi odpowiadać treści SIWZ. Oferta musi być sporządzona w języku polskim, na piśmie wg załączonych do SIWZ wzorów druków (formularz ofertowy) oraz zawierać pozostałe dokumenty wskazane w wykazie załączników 1 2 SIWZ.
- Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ.
- Zamawiający może w każdym czasie przed terminem składania ofert zmodyfikować treść SIWZ, powiadamiając niezwłocznie o zmianie treści wszystkich wykonawców, którzy pobrali SIWZ.
- Zamawiający odrzuci ofertę w przypadkach przewidzianych w art. 89 ust. 1 ustawy.
- Zamawiający unieważni postępowanie w przypadkach określonych w art. 93 ust 1 i 2 Ustawy. O unieważnieniu postępowania o udzielenie zamówienia Zamawiający zawiadomi równocześnie wszystkich Wykonawców, którzy:
    1. ubiegali się o udzielenie zamówienia – w przypadku unieważnienia postępowania przed upływem terminu składania ofert
    2. złożyli oferty – w przypadku unieważnienia postępowania po upływie terminu składania ofert

  podając uzasadnienia faktyczne i prawne.

- Wykluczenie wykonawcy z postępowania o udzielenie zamówienia nastąpi z art.24 ust.1 i 2. Ofertę wykonawcy wykluczonego uznaje się za odrzuconą. O odrzuceniu ofert zamawiający zawiadomi wszystkich wykonawców.

3. **Sposób składania ofert, wycofanie ofert, wnoszenie zmian do złożonych ofert**

- Wykonawca winien umieścić ofertę w kopercie zaadresowanej na Zamawiającego na adres:
  INSTYTUT BADAŃ SYSTEMOWYCH PAN
  01-447 Warszawa ul. Newelska 6
  z dopiskiem PRZETARG FIREWALL
- Wykonawca może wprowadzać zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmian, poprawek itp. Przed terminem składania ofert. W tym celu Wykonawca powinien złożyć Zamawiającemu kolejną zamkniętą kopertę, oznaczona jak wyżej z dopiskiem „Zmiana" lub „Wycofanie"
- Wykonawca nie może wprowadzać jakichkolwiek zmian w treści oferty po upływie terminu składania ofert
- Ofertę złożoną po terminie Zamawiający zwróci bez otwierania.
- Dokumenty winny być wykonane w języku polskim.

4. **Miejsce oraz termin składania i otwarcia ofert**
Miejsce składania i otwarcia ofert:

Termin składania ofert: 15.09.2010 r., godz. 12:00 Instytut Badań Systemowych PAN 01-447 Warszawa ul. Newelska 6 Kancelaria.

Termin i miejsce otwarcia ofert 15.09.2010 r.godz. 12:15 INSTYTUT BADAŃ SYSTEMOWYCH PAN 01-447 Warszawa ul. Newelska 6 pok. 200

Wykonawcy mogą uczestniczyć w publicznej sesji otwarcia ofert. W przypadku nieobecności wykonawcy przy otwieraniu ofert, Zamawiający prześle wykonawcy informację z otwarcia ofert na jego pisemny wniosek.

5. **Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty**

Najniższa cena**.**

6. **Informacja o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego**
Jeżeli Zamawiający dokona wyboru oferty, umowa w sprawie realizacji zamówienia publicznego zostanie zawarta z wykonawcą, który spełni wszystkie przedstawione wymagania oraz, którego oferta okaże się najkorzystniejsza.
O miejscu i dokładnym terminie zawarcia umowy Zamawiający powiadomi niezwłocznie wybranego Wykonawcę.

7. **Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy**
   Wykonawca, który przedstawił najniższą cenę, będzie zobowiązany do podpisania umowy.

8. **Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia.**
   Uczestnikom postępowania, których interes prawny w uzyskaniu zamówienia doznał lub mógł doznać uszczerbku w wyniku naruszenia przez Zamawiającego przepisów ustawy przysługują środki ochrony prawnej na podstawie art. 179 - 198 ustawy Prawo zamówień publicznych.

9. **Opis części zamówienia**
   Zamawiający dopuszcza składanie ofert częściowych

10. **Maksymalną liczbę wykonawców, z którymi zamawiający zawrze umowę ramową, jeżeli zamawiający przewiduje zawarcie umowy ramowej**
    Zamawiający nie przewiduje zawarcia umowy ramowej.

11. **Informację o przewidywanych zamówieniach uzupełniających, o których mowa w art. 67 ust. 1 pkt 6 i 7 lub art. 134 ust. 6 pkt 3**
    Zamawiający nie przewiduje zamówień uzupełniających.

12. **Oferty wariantowe**
    Wykonawca ma prawo złożyć tylko jedna ofertę.

13. **Adres poczty elektronicznej lub strony internetowej zamawiającego**
    Adresy poczty elektronicznej - jak podano w punkcie 9. Informacje o sposobie porozumiewania się zamawiającego z wykonawcami, a także wskazanie osób uprawnionych do porozumiewania się z wykonawcami.

14. **Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między zamawiającym a wykonawcą**
    Zamawiający nie przewiduje rozliczenia w walutach obcych.

15. **Aukcja elektroniczna**
    Zamawiający nie przewiduje aukcji elektronicznej.

16. **Wysokość zwrotu kosztów udziału w postępowaniu**
    Zamawiający nie przewiduje żadnego zwrotu kosztów w postępowaniu.

Lista załączników (załączniki stanowią integralną część SIWZ):

1. Formularz ofertowy - załącznik nr 1
2. Oświadczenie o spełnianiu wymogów z art. 22 ust. 1 ustawy - załącznik nr 2

Załącznik nr 1

.....
Pieczęć Wykonawcy (miejscowość, data)

Instytut Badań Systemowych PAN
01-447 Warszawa ul. Newelska 6

FORMULARZ OFERTOWY

W związku z ogłoszonym przetargiem nieograniczonym na: modernizację instalacji elektrycznej w budynku IBS PAN

Dotyczy części pierwszej:
Oferujemy dostawę przedmiotu zamówienia za następującą cenę ofertową brutto:…… zł (słownie: ……)
Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia, akceptujemy ją w całości i nie wnosimy do niej zastrzeżeń oraz przyjmujemy wszystkie warunki do stosowania.
Dotyczy części drugiej:
Oferujemy dostawę przedmiotu zamówienia za następującą cenę ofertową brutto:…… zł (słownie: ……)
Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia, akceptujemy ją w całości i nie wnosimy do niej zastrzeżeń oraz przyjmujemy wszystkie warunki do stosowania.
Dotyczy części trzeciej:
Oferujemy dostawę przedmiotu zamówienia za następującą cenę ofertową brutto:…… zł (słownie: ……)
Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia, akceptujemy ją w całości i nie wnosimy do niej zastrzeżeń oraz przyjmujemy wszystkie warunki do stosowania.

1. Oświadczamy, że znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia, określonej jako możliwość dysponowania lub dostępu do środków finansowych wystarczających do realizacji zamówienia bez udzielania zaliczki, z uwzględnieniem zobowiązań z tytułu realizacji innych zamówień,

2. Oświadczamy, że uważamy się za związanych niniejszą ofertą przez okres **30 dni**, licząc od upływu terminu składania ofert.

3. W przypadku przyznania nam zamówienia, zobowiązujemy się do zawarcia umowy w miejscu i terminie wskazanym przez Zamawiającego.

4. Ofertę złożono na ..... stronach kolejno ponumerowanych.

5. Integralną część oferty stanowią następujące dokumenty **):

1) .....

2) .....

3) .....

4) .....

5) .....

6) .....

7) .....

8) .....

.....

podpis osoby/osób
upoważnionej/upoważnionych
do reprezentowania wykonawcy

Uwaga:

***** niepotrzebne skreślić

****)** jeżeli dołączone są odpisy dokumentów lub ich kserokopie, to muszą być poświadczone za zgodność z oryginałem przez osobę (osoby) podpisującą ofertę.

Załącznik Nr 2

/pieczęć wykonawcy/

Zamawiający:

Instytut Badań Systemowych PAN
01-447 Warszawa
ul. Newelska 6

OŚWIADCZENIE

Złożone zgodnie z art. 22 ust. 1 i art. 24 ust. 1 i 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2004 r. Nr 19, poz. 177 z późn. zm.)

WYKONAWCA:
.....

ADRES:
.....

przystępując do udziału w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, którego przedmiotem jest: modernizacja instalacji elektrycznej w budynku IBS PAN
oświadcza, że:

1) posiadamy uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień;
2) posiadamy niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia;
3) znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia;
4) nie podlegamy wykluczeniu z postępowania o udzielenie zamówienia, na podstawie art. 24 ust. 1 i 2, który stanowi, że:

Z ubiegania się o udzielenie zamówienia publicznego wyklucza się:

1) *wykonawców, którzy w ciągu ostatnich 3 lat przed wszczęciem postępowania wyrządzili szkodę niewykonując zamówienia lub wykonując je nienależycie, a szkoda ta nie została dobrowolnie naprawiona do dnia wszczęcia postępowania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które wykonawca nie ponosi odpowiedzialności;*
2) *wykonawców, w stosunku do których otwarto likwidację lub których upadłość ogłoszono, z wyjątkiem wykonawców, którzy po ogłoszeniu upadłości zawarli układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli poprzez likwidację majątku upadłego,*
3) *wykonawców, którzy zalegają z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, z wyjątkiem przypadków gdy uzyskali oni przewidziane prawem zwolnienie, odroczenie, rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu;*
4) *osoby fizyczne, które prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,*
5) *spółki jawne, których wspólnika prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę*

zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,

6) *spółki partnerskie, których partnera lub członka zarządu prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,*
7) *spółki komandytowe oraz spółki komandytowo-akcyjne, których komplementariusza prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,*
8) *osoby prawne, których urzędującego członka organu zarządzającego prawomocnie skazano za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przeciwko prawom osób wykonujących pracę zarobkową, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych, a także za przestępstwo skarbowe lub przestępstwo udziału w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa lub przestępstwa skarbowego,*
9) *podmioty zbiorowe, wobec których sąd orzekł zakaz ubiegania się o zamówienia, na podstawie przepisów o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary;*
10) *wykonawców, którzy nie spełniają warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 pkt 1-3.*

Z postępowania o udzielenie zamówienia wyklucza się również wykonawców, którzy:

1) *wykonywali bezpośrednio czynności związane z przygotowaniem prowadzonego postępowania, lub posługiwali się w celu sporządzenia oferty osobami uczestniczącymi w dokonywaniu tych czynności, chyba że udział tych wykonawców w postępowaniu nie utrudni uczciwej konkurencji: przepisu nie stosuje się do wykonawców, którym udziela się zamówienia na podstawie art. 62 ust. 1 pkt 2 lub art. 67 ust. 1 pkt 1 i 2;*
2) *złożyli nieprawdziwe informacje mające wpływ na wynik prowadzonego postępowania;*
3) *nie złożyli oświadczenia o spełnianiu warunków udziału w postępowaniu lub dokumentów potwierdzających spełnianie tych warunków lub złożone dokumenty zawierają błędy, z zastrzeżeniem art. 26 ust. 3;*
4) *nie wnieśli wadium, w tym również na przedłużony okres związania ofertą, lub nie zgodzili się na przedłużenie okresu związania ofertą.*

Miejscowość, ..., dnia .....

.....
podpis osoby/osób
upoważnionej/upoważnionych
do reprezentowania wykonawcy