SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

W POSTĘPOWANIU O ZAMÓWIENIE PUBLICZNE
W TRYBIE

PRZETARGU NIEOGRANICZONEGO
POWYŻEJ RÓWNOWARTOŚCI 137.000 EURO
NA

MODERNIZACJĘ WĘZŁA CENTRALNEGO SIECI ROZLEGŁEJ
INSTYTUTU PAMIĘCI NARODOWEJ

nr 72532000-3 , nr 30230000-0, nr 30242100-8, nr 30244000-1
Wspólnego Słownika Zamówień (CPV)

ZAMAWIAJĄCY:

INSTYTUT PAMIĘCI NARODOWEJ – KOMISJA ŚCIGANIA ZBRODNI PRZECIWKO NARODOWI POLSKIEMU
PL. KRASIŃSKICH 2/4/6
00-207 WARSZAWA

Niniejsze postępowanie jest prowadzone na podstawie przepisów ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2006 r. Nr 164, poz. 1163 ze zm.).

I. INFORMACJE O ZAMAWIAJĄCYM.

Zamawiającym w niniejszym postępowaniu jest:
Instytut Pamięci Narodowej – Komisja Ścigania Zbrodni przeciwko Narodowi Polskiemu, Pl. Krasińskich 2/4/6, 00 – 207 Warszawa,
Adres korespondencyjny: ul. Towarowa 28, 00-839 Warszawa

II. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

1) wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje w toku postępowania o udzielenie zamówienia publicznego mogą być przekazywane **faksem lub pisemnie,**
2) osobami uprawnionymi do kontaktu z Wykonawcami są:
   - w sprawach technicznych – Krzysztof Lenart w godz. 9.00 – 15.00 tel. (0-22) 581-88-99,
   - w sprawach procedury postępowania o udzielenie zamówienia publicznego – Adriana Urbanik w godz. 9.00 – 15.00 tel. (0-22) 581-88-04, fax. (0-22) 581-88-14.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia stanowi:

MODERNIZACJA WĘZŁA CENTRALNEGO SIECI ROZLEGŁEJ INSTYTUTU PAMIĘCI NARODOWEJ

Nie dopuszcza się złożenia ofert częściowych oraz wariantowych.

Szczegółowy opis przedmiotu zamówienia:

Przedmiot zamówienia stanowi modernizacja węzła centralnego sieci rozległej WAN tj. zakup wraz z instalacją, konfiguracją i integracją z infrastrukturą sieciową Zamawiającego następujących urządzeń sieciowych i oprogramowania:
- dwóch modularnych przełączników rdzeniowych,
- firewalla (główna zapora sieciowa),
- systemu antywirusowego,
- automatycznego systemu analizy i zapobiegania zagrożeń IPS (sonda IPS),
- oprogramowania do analizy i zarządzania siecią oraz urządzeniami,
- dwudziestu trzech routerów z możliwością analizy ruchu oraz zarządzania pasmem.

Opis instalacji, konfiguracji oraz integracji z istniejącą infrastrukturą teleinformatyczną:

Na cały okres wdrożenia ze strony Zamawiającego oraz Wykonawcy zostaną wyznaczone osoby, pełniące rolę *Kierownika projektu*, odpowiedzialne za kontakty i ustalania pomiędzy Zamawiającym a Wykonawcą.

Dostawa sprzętu nastąpi wg załącznika nr 3 „Wykaz lokalizacji i miejsc dostawy urządzeń”**.**

Wykaz lokalizacji w których prowadzone będzie wdrożenie ujęty jest w załączniku nr 4 o nazwie „Wykaz miejsc instalacji, konfiguracji i integracji urządzeń”. Usługa wdrożenia będzie obejmowała swoim zakresem, fizyczną instalację wszystkich urządzeń będących przedmiotem postępowania (w miejscach wskazanych przez Zamawiającego), instalację oprogramowania na maszynach serwerowych wskazanych przez Zamawiającego, integrację z istniejącą siecią oraz konfigurację całego systemu zgodnie z wytycznymi Biura Organizacyjnego IPN.

Usługa konfiguracji będzie obejmowała:

- instalację urządzeń zgodnie ze strukturą sieci (LAN oraz WAN) przygotowaną przez Zamawiającego (zostanie przekazana Wykonawcy na początkowym etapie wdrożenia).
- podstawową konfigurację wszystkich urządzeń zgodnie z ogólnie przyjętym schematem w sieci IPN (szczegóły zostaną przekazane na początkowym etapie wdrożenia).
- zaawansowaną konfigurację całego systemu obejmującą platformę komunikacyjną, bezpieczeństwo urządzeń, bezpieczeństwo sieci LAN oraz sieci WAN, wdrożenie oprogramowania do zarządzania infrastrukturą sieciową.

Ostateczne ustalenia z Zamawiającym dotyczące realizacji całego projektu zostaną opisane przez Wykonawcę w dokumencie projektowym, który będzie zawierał szczegóły konfiguracyjne. Dokument zostanie następnie uzgodniony z Zamawiającym. Akceptacja dokumentu ze strony Zamawiającego będzie warunkiem koniecznym do zainicjowania etapu wdrożenia.

Wykonawca po zakończeniu wdrożenia przekaże Zamawiającemu dokumentację powykonawczą systemu.

Oba dokumenty tj. „Dokumentacja projektowa" oraz „Dokumentacja powykonawcza" pełnią rolę oficjalnych dokumentów wdrożeniowych po pisemnej akceptacji ze strony Zamawiającego.

Prowadzone prace wdrożeniowe i instalacyjne nie mogą zakłócać prawidłowej pracy istniejącej sieci. Wszystkie konieczne przerwy w pracy systemu muszą być zgłoszone najpóźniej na 24 godziny przed planowaną przerwą i powinny mieć miejsce poza godzinami pracy (tj. poza 8:15-16:15 w dni robocze od poniedziałku do piątku).

Opis parametrów technicznych sprzętu i oprogramowania został szczegółowo określony w załączniku nr 2 do specyfikacji.

Zamawiający nie dopuszcza powierzenia wykonania przedmiotu zamówienia w całości lub części podwykonawcom.

IV. WARUNKI UCZESTNICTWA W POSTĘPOWANIU:

W postępowaniu mogą wziąć udział Wykonawcy, którzy spełniają następujące warunki:

1. Podmiotowe:

1. spełniają warunki określone w art. 22 ust. 1 ustawy Prawo zamówień publicznych,
2. są uprawnieni do występowania w obrocie prawnym w zakresie objętym zamówieniem,
3. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia – posiadają ubezpieczenie od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej w zakresie objętym zamówieniem na kwotę nie mniejszą niż wartość oferty brutto w zł. (w przypadku składnia oferty przez Wykonawców ubiegających się wspólnie o udzielenie zamówienia, na podstawie art. 23 Ustawy PZP warunek ten musi być spełniony co najmniej przez jednego z Wykonawców lub łącznie przez kilku lub wszystkich Wykonawców),

2. Inne:

1. dostarczą przedmiot zamówienia fabrycznie nowy,
2. zapewnią minimum 12-miesięczną gwarancję opartą na gwarancji producenta na dostarczany sprzęt – o ile wymagania szczegółowe nie specyfikują inaczej,
3. oprogramowanie powinno być dostarczone z minimum rocznym wsparciem producenta - o ile wymagania szczegółowe nie specyfikują inaczej.

Ocena spełnienia warunków udziału w postępowaniu zostanie dokonana metodą „spełnia – nie spełnia" w oparciu o dokumenty, oświadczenia i informacje zawarte w ofercie. Z treści załączonych dokumentów musi jednoznacznie wynikać, że stawiane warunki Wykonawca spełnił**.** Niespełnienie warunków określonych w pkt 1 skutkować będzie **wykluczeniem z postępowania** a w przypadku warunków określonych w pkt 2 **odrzuceniem oferty.**

V. DOKUMENTY/OŚWIADCZENIA JAKIE MAJĄ DOSTARCZYĆ WYKONAWCY W CELU POTWIERDZENIA SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ ŻE OFEROWANA DOSTAWA/USŁUGA JEST ZGODNA Z WYMAGANIAMI OKREŚLONYMI PRZEZ ZAMAWIAJĄCEGO A TAKŻE INNE WYMAGANE DOKUMENTY.

Wykonawcy:

1) dołączą do oferty formularz ofertowy **(załącznik nr 1 do specyfikacji),**
2) dołączą do oferty oferowane parametry techniczne **(załącznik nr 2 do specyfikacji):**
   - w stosunku do oferowanego sprzętu i oprogramowania specyfikacja techniczna musi zawierać wszystkie elementy oferowanego rozwiązania (włącznie z numerami katalogowymi producentów), tym samym umożliwiając jednoznaczną weryfikację warunków wymaganych w SIWZ,
3) dołączą do oferty oświadczenie o spełnianiu warunków z art. 22 ust. 1 ustawy Prawo zamówień publicznych **(załącznik nr 3 do specyfikacji),**
4) dołączą do oferty polisę, a w przypadku jej braku inny dokument potwierdzający, że wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności – z dokumentu powinno wynikać posiadanie przez Wykonawcę ubezpieczenia od odpowiedzialności cywilnej w zakresie prowadzonej działalności gospodarczej w zakresie przedmiotu zamówienia na kwotę nie mniejszą niż wartość oferty brutto w zł,
5) dołączą do oferty zaświadczenie niezależnego podmiotu zajmującego się poświadczaniem zgodności działań Wykonawcy z normami jakościowymi, jeżeli zamawiający odwołuje się do systemów zapewnienia jakości opartych na odpowiednich normach europejskich - Certyfikat ISO 9001 lub równoważny na proces projektowania i produkcji oferowanego sprzętu,
6) dołączą do oferty oświadczenie producentów lub polskich przedstawicielstw producentów o posiadaniu przez wykonawcę autoryzacji do sprzedaży, instalacji oraz konfiguracji ich rozwiązań na terenie Polski – dotyczy sprzętu,
7) dołączą do oferty oświadczenie producentów lub polskich przedstawicielstw producentów o posiadaniu przez wykonawcę autoryzacji do sprzedaży, instalacji oraz konfiguracji ich rozwiązań na terenie Polski – dotyczy oprogramowania,
8) dołączą do oferty aktualny odpis z właściwego rejestru albo aktualnego zaświadczenia o wpisie do ewidencji działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub zgłoszenia do ewidencji działalności gospodarczej, wystawionego nie wcześniej niż **6 miesięcy** przed upływem terminu składania ofert,
9) dołączą do oferty parafowany projekt umowy, stanowiący **załącznik nr 4 do specyfikacji**.

Wymienione powyżej w pkt 1 i 3 dokumenty wchodzące w skład oferty winny być przedstawione w formie oryginałów, pozostałe oryginałów lub poświadczonych za zgodność z oryginałem kopii.

Zgodność z oryginałem wszystkich kopii dokumentów wchodzących w skład oferty musi być potwierdzona przez przedstawiciela Wykonawcy lub pełnomocnika (zgodnie z dokumentem określającym status prawny Wykonawcy lub dołączonym do oferty pełnomocnictwem).

VI. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1) każdy Wykonawca może złożyć tylko jedną ofertę,
2) ofertę należy przygotować zgodnie z zaleceniami określonymi w niniejszej specyfikacji,
3) oferta musi być podpisana przez osoby upełnomocnione do reprezentowania Wykonawcy i zaciągania w jego imieniu zobowiązań finansowych w wysokości odpowiadającej cenie oferty,
4) pełnomocnictwo osób podpisujących ofertę do reprezentowania Wykonawcy, zaciągania w jego imieniu zobowiązań finansowych w wysokości odpowiadającej cenie oferty oraz podpisania oferty musi bezpośrednio wynikać z dokumentów dołączonych do oferty; oznacza to, że jeżeli pełnomocnictwo takie nie wynika wprost z dokumentu stwierdzającego status prawny Wykonawcy (odpisu z właściwego rejestru lub zaświadczenia o wpisie do ewidencji działalności gospodarczej) to do oferty należy dołączyć **oryginał pełnomocnictwa** wystawionego na reprezentanta Wykonawcy przez osoby do tego upełnomocnione,
5) wzory dokumentów dołączonych do niniejszej specyfikacji powinny zostać wypełnione przez

Wykonawcę i dołączone do oferty bądź też przygotowane przez Wykonawcę w innej, zgodnej z niniejszą specyfikacją formie,

6) żadne dokumenty wchodzące w skład oferty, w tym również te przedstawiane w formie oryginałów, nie podlegają zwrotowi przez Zamawiającego,
7) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty,
8) podana w ofercie cena ofertowa musi zawierać wszelkie koszty jakie poniesie Wykonawca z tytułu należytej, zgodnej z załączonym wzorem umowy oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia,
9) wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje w toku postępowania o udzielenie zamówienia publicznego mogą być przekazywane faksem lub pisemnie.

Warunki dotyczące konsorcjum

1. W odniesieniu do wymagań postawionych przez Zamawiającego, każdy z Wykonawców wchodzący w skład konsorcjum musi **oddzielnie** udokumentować, że nie podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 1-9 ustawy Prawo zamówień publicznych. W pozostałym zakresie konsorcjum może złożyć **jeden wspólny dokument.**
2. Oferta musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich Wykonawców występujących wspólnie.
3. Wykonawcy występujący wspólnie muszą ustanowić pełnomocnika (lidera) do reprezentowania ich w postępowaniu o udzielenie niniejszego zamówienia lub reprezentowania ich w postępowaniu oraz zawarcia umowy o udzielenie przedmiotowego zamówienia publicznego. Umocowanie może wynikać z treści umowy konsorcjum lub zostać przedłożone oddzielnie wraz z ofertą.
4. Wszelka korespondencja prowadzona będzie wyłącznie z pełnomocnikiem (liderem).
5. Wypełniając formularz ofertowy, składając oświadczenie o spełnianiu warunków udziału w postępowaniu, jak również wypełniając inne dokumenty powołujące się na „Wykonawcę", w miejscu np. nazwa i adres Wykonawcy należy wpisać dane konsorcjum (wymienić wszystkich Wykonawców wspólnie ubiegających się o zamówienie).

VII. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca pozostaje związany złożoną ofertą przez 60 dni.
Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

VIII. TERMIN WYKONANIA ZAMÓWIENIA

Termin wykonania zamówienia wynosi:
I etap – dostawa urządzeń sieciowych i oprogramowania - w ciągu **45 dni od daty zawarcia umowy,**
II etap – opracowanie projektu wdrożenia – instalacji, konfiguracji i integracji, uzgodnienie dokumentu projektowego z zamawiającym, wykonanie wdrożenia oraz dokumentacji powykonawczej **do dnia 15 grudnia 2007 r.**

IX. KRYTERIA OCENY OFERT I ICH ZNACZENIE

Oceny ofert dokona zgodnie z podanym kryterium i zasadami komisja przetargowa IPN powołana przez Zamawiającego.
W odniesieniu do Wykonawców, którzy spełnili postawione warunki formalne, komisja przetargowa IPN dokona oceny ich ofert.

Kryterium	Max. liczba punktów	Wagi %

Cena	100	100

W ofercie należy podać cenę netto oraz cenę brutto. Cena winna zawierać wszelkie koszty jakie poniesie Wykonawca w związku z realizacją przedmiotu zamówienia.

Liczba punktów za cenę oferty ocenianej będzie wyliczana według następującego wzoru:

$$C = \frac{Cmin}{Ci} \text{ x } 100 \text{ x } 100\ \%$$

C – ilość otrzymanych punktów za dane kryterium
Cmin –najniższa cena spośród ofert nie odrzuconych
Ci – cena oferty badanej

Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą sumę punktów.

X. WADIUM

Każdy Wykonawca zobowiązany jest zabezpieczyć swą ofertę wadium w wysokości 22.000 zł (słownie: dwadzieścia dwa tysiące złotych).

Oferta, która przed upływem terminu składania ofert nie zostanie zabezpieczona akceptowaną przez Zamawiającego formą wadium w wymaganej wysokości a także oferta nie posiadająca dołączonego dokumentu potwierdzającego wniesienie wadium przez Wykonawcę zostanie odrzucona.

1. **Forma wadium**.
   Wadium może być wniesione wyłącznie w następujących formach:
   a) pieniądzu,
   b) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym,
   c) gwarancjach bankowych,
   d) gwarancjach ubezpieczeniowych,
   e) w poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. Nr 109, poz. 1158, z późn. zm.).

Wszelkie rozliczenia związane z realizacją zamówienia publicznego którego dotyczy niniejsza specyfikacja dokonywane będą wyłącznie w złotych polskich (PLN).
Wadium wnoszone w innej niż pieniądz formie musi posiadać ważność co najmniej do końca terminu związania Wykonawcy złożoną przez niego ofertą. Wniesienie wadium o krótszym terminie ważności skutkować będzie odrzuceniem oferty.

2. **Miejsce i sposób wniesienia wadium.**
   Wadium wnoszone w pieniądzu należy **przelać na rachunek** Zamawiającego: NBP o/o w Warszawie 60101010100092921391200000.

   Wadium wnoszone w innych dopuszczonych przez Zamawiającego formach należy złożyć w oryginale w kasie: Pl. Krasińskich 2/4/6 pokój 2K06 w godz. 12°°- 14°°, a do oferty dołączyć kopię dokumentu posiadającą potwierdzenie złożenia w kasie dokonane przez kasjera.

3. **Termin wniesienia wadium.**
   Wadium należy wnieść przed upływem terminu składania ofert, przy czym wniesienie wadium w pieniądzu za pomocą przelewu bankowego Zamawiający będzie uważał za **skuteczne tylko wówczas gdy przed upływem terminu składania ofert** Wykonawca przedłoży potwierdzenie dokonania wpłaty.

X. ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

1. Zamawiający żąda zabezpieczenie należytego wykonania umowy w wysokości 10% całkowitej ceny ofertowej .
2. Zabezpieczenie musi być wniesione przez Wykonawcę przed zawarciem umowy w jednej z następujących form:
   1) pieniężnej – **przelewem na rachunek** Zamawiającego: NBP o/o w Warszawie 60101010100092921391200000,
   2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym,
   3) gwarancjach bankowych,
   4) gwarancjach ubezpieczeniowych,
   5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt. 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
3. Gwarancja i poręczenie muszą być nieodwołalne, bezwarunkowe, zapewniające płatność na rzecz Zamawiającego na każde żądanie bez konieczności przedkładania dodatkowych dokumentów, muszą zawierać rezygnację gwaranta z podnoszenia zarzutów (art. 883 k.c.), włącznie z wykluczeniem możliwości potrącenia oraz zarzutem możliwości uchylenia się od skutków prawnych błędnego oświadczenia, z wyjątkiem uchylenia się od skutków prawnych oświadczenia, zgodnie z art. 86 k.c. oraz muszą obejmować rezygnację z prawa do zdeponowania kwoty gwarancji i poręczenia. Zamawiający zastrzega sobie prawo akceptacji treści gwarancji i poręczenia.
   UWAGA: wypłata z gwarancji nie może być uzależniona od zgłoszenia żądania wypłaty za pośrednictwem banku Zamawiającego, który to bank potwierdzi, że podpisy na żądaniu wypłaty zostały złożone przez osoby upoważnione do zaciągania zobowiązań majątkowych w imieniu Zamawiającego.
4. Zabezpieczenie służy zaspokojeniu wszelkich roszczeń Zamawiającego z tytułu nie wykonania lub nienależytego wykonania postanowień umowy przez Wykonawcę. W szczególności z zabezpieczenia Zamawiający ma prawo pokryć kary umowne.
5. Zabezpieczenie podlega zwolnieniu przez Zamawiającego w wysokości 70% sumy zabezpieczenia w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane (dokonania ostatniego odbioru przedmiotu zamówienia), a 30 % tej sumy w terminie 14 dni od dnia kończącego okres gwarancyjny.

XI. MIEJSCE, TERMIN I SPOSÓB SKŁADANIA I OTWARCIA OFERT.

1. Ofertę należy złożyć w centrali Zamawiającego: **ul. Towarowa 28, 00-839 Warszawa pokój nr 1 - parter - Kancelaria**

   do dnia 3 października 2007 r., godz. 10.00

2. Oferta złożona po terminie zostanie zwrócona Wykonawcy bez otwierania.
3. Ofertę należy złożyć w dwóch nieprzeźroczystych, zabezpieczonych przed otwarciem kopertach - wewnętrznej i zewnętrznej. Kopertę zewnętrzną należy opisać następująco (uzupełniając miejsca wykropkowane):

   Instytut Pamięci Narodowej
   Komisja Ścigania Zbrodni Przeciwko
   Narodowi Polskiemu
   Plac Krasińskich 2/4/6 00-207 Warszawa

   Oferta w postępowaniu na modernizację węzła centralnego sieci rozległej IPN
   Nie otwierać przed dniem 3 października 2007 r., godz. 10.15

4. Na kopercie wewnętrznej, w której winna znajdować się oferta oprócz opisu jw. należy umieścić **nazwę i adres Wykonawcy.**
5. Otwarcie ofert nastąpi w centrali Zamawiającego: **ul. Towarowa 28, 00-839 Warszawa pokój nr 603 -**

VI piętro (Wydział Zamówień Publicznych) dnia 3 października 2007 r., godz. 10.15.

XII. ZMIANY LUB WYCOFANIE ZŁOŻONEJ OFERTY.

1. **Skuteczność zmian lub wycofania złożonej oferty** - Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę. Zmiany lub wycofanie złożonej oferty są skuteczne tylko wówczas gdy zostały dokonane przed upływem terminu składania ofert.
2. **Zmiana złożonej oferty** - zmiany, poprawki lub modyfikacje złożonej oferty muszą być złożone w miejscu i według zasad obowiązujących przy składaniu oferty. Odpowiednio opisane koperty (wewnętrzną i zewnętrzną) zawierające zmiany należy dodatkowo opatrzyć dopiskiem "ZMIANA".
3. **Wycofanie złożonej oferty** - wycofanie złożonej oferty następuje poprzez złożenie pisemnego powiadomienia podpisanego przez upełnomocnionego przedstawiciela Wykonawcy. Powiadomienie należy złożyć w miejscu i według zasad obowiązujących przy składaniu oferty. Odpowiednio opisane koperty (wewnętrzną i zewnętrzną) zawierające powiadomienie należy dodatkowo opatrzyć dopiskiem "WYCOFANIE".

XIII. WYBÓR OFERTY I ZAWIADOMIENIE O WYNIKU POSTĘPOWANIA

1. Przy dokonywaniu wyboru oferty Zamawiający stosował będzie wyłącznie zasady i kryterium określone w niniejszej specyfikacji.
2. Za najkorzystniejszą uznana zostanie ta z ocenianych ofert, która po dokonaniu oceny zgodnie z przyjętym kryterium i zasadami oceny ofert uzyska najwyższą liczbę punktów.
3. Zamawiający udzieli zamówienia Wykonawcy, którego oferta zostanie uznana za najkorzystniejszą.
4. Miejsce i termin podpisania umowy zostanie określony Wykonawcy, którego ofertę wybrano w piśmie zawiadamiającym o wyborze.

XIV. SPOSÓB I TERMIN PŁATNOŚCI

1. Za dostarczone produkty i wykonane usługi płatność zostanie zrealizowana po ich odbiorze potwierdzonym protokołem dostawy – zgodnie z § 7 projektu umowy.
2. Płatność może zostać uruchomiona po zatwierdzeniu protokołu dostawy przez Zamawiającego.
3. Zapłata nastąpi przelewem w ciągu 14 dni od daty otrzymania faktury VAT, potwierdzonej protokołem dostawy.

XV. INFORMACJE DOTYCZĄCE WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Zamawiający nie dopuszcza podania ceny ofertowej i jej elementów w walutach obcych. Cena winna być podana w walucie polskiej (w złotych i groszach).

XVI. ZMIANY W TREŚCI SPECYFIKACJI

W szczególnie uzasadnionych przypadkach Zamawiający może w każdym czasie, przed upływem terminu składania ofert zmodyfikować treść niniejszej specyfikacji. Informację o wprowadzonych w ten sposób modyfikacjach Zamawiający przekaże niezwłocznie wszystkim Wykonawcom. Modyfikacje są każdorazowo wiążące dla Wykonawców.

XVII. ŚRODKI ODWOŁAWCZE PRZYSŁUGUJĄCE WYKONAWCOM

Wykonawcy w toku postępowania o udzielenie zamówienia publicznego przysługują środki ochrony prawnej przewidziane w ustawie z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2006 r. Nr 164, poz. 1163 ze zm.).

XVIII. FORMALNOŚCI KTÓRYCH NALEŻY DOPEŁNIĆ PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY

1. Zamawiający zawrze umowę o wykonanie zamówienia w terminie nie krótszym niż 7 dni od dnia przekazania zawiadomienia o wyborze oferty, nie później niż przed upływem terminu związania ofertą.
2. Umowa będzie zawierana w centrali Zamawiającego w Warszawie przy ul. Towarowej 28.
3. Umowa zostanie zawarta według wzoru, stanowiącego **załącznik nr 4** do specyfikacji.
4. W celu zawarcia umowy Wykonawca, którego oferta zostanie wybrana, będzie zobowiązany do wskazania Zamawiającemu osób, które będą w jego imieniu zawierać umowę oraz do ewentualnego przekazania oryginałów stosownych pełnomocnictw tych osób do zawarcia umowy.

XIX. SPOSÓB UDZIELANIA WYJAŚNIEŃ DOTYCZĄCYCH SPECYFIKACJI.

Wykonawca w trakcie postępowania może zwrócić się do Zamawiającego z prośbą o udzielenie wyjaśnień dotyczących treści i postanowień niniejszej specyfikacji. Prośbę taką należy sformułować na piśmie i przekazać Zamawiającemu nie później niż 6 dni przed upływem terminu składania ofert. Zapytania skierowane po w/w terminie lub skierowane w innej formie niż pisemna nie będą rozpatrywane.
Zamawiający niezwłocznie udzieli pisemnych wyjaśnień powiadamiając wszystkich Wykonawców którym doręczono niniejszą specyfikację o treści zapytania bez ujawniania jego źródła.

XX. INNE INFORMACJE

Zamawiający nie przewiduje: aukcji elektronicznej, zawarcia umowy ramowej, zamówień uzupełniających, zwrotu kosztów udziału w postępowaniu.

XXI. ZAŁĄCZNIKI

1. **załącznik nr 1** – wzór formularza ofertowego,
2. **załącznik nr 2** – opis przedmiotu zamówienia:
   TABELA 1 – Przełącznik rdzeniowy (2 szt),
   TABELA 2 – Główna zapora sieciowa (1 szt),
   TABELA 3 – Sonda IPS (1 szt),
   TABELA 4 – System antywirusowy (1 szt),
   TABELA 5 – Oprogramowanie do zarządzania siecią (1 szt),
   TABELA 6 – Router centralny WAN (1 szt),
   TABELA 7 – Routery oddziałowe typ I (13 szt),
   TABELA 8 – Routery oddziałowe typ II (9 szt).
3. **załącznik nr 3** – Wykaz lokalizacji i miejsc dostawy urządzeń,
4. **załącznik nr 4 –** Wykaz miejsc instalacji, konfiguracji i integracji urządzeń,
5. **załącznik nr 5 -** wzór oświadczenia Wykonawcy o spełnianiu przez niego warunków określonych w art. 22 ust. 1 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2006 r. Nr 164, poz. 1163 ze zm.),
6. **załącznik nr 6** – wzór umowy.

Załącznik nr 1 do specyfikacji istotnych warunków zamówienia w postępowaniu o zamówienie publiczne na modernizację węzła centralnego sieci rozległej IPN

Formularz ofertowy

ZAMAWIAJĄCY: **WYKONAWCA:**

INSTYTUT PAMIĘCI NARODOWEJ
KOMISJA ŚCIGANIA ZBRODNI
PRZECIWKO NARODOWI POLSKIEMU
Pl. Krasińskich 2/4/6, ...
00-207 Warszawa ***pieczęć Wykonawcy***

Składamy ofertę na:

MODERNIZACJĘ WĘZŁA CENTRALNEGO SIECI ROZLEGŁEJ INSTYTUTU PAMIĘCI NARODOWEJ

Oferujemy modernizację węzła centralnego sieci rozległej IPN :

I etap – dostawa urządzeń sieciowych i oprogramowania - w ciągu 45 dni od daty zawarcia umowy za cenę netto .....PLN plus podatek VAT w kwocie ..... co daje cenę brutto ..... PLN (słownie: .....),

II etap – opracowanie projektu wdrożenia – instalacji, konfiguracji i integracji, uzgodnienie dokumentu projektowego z zamawiającym, wykonanie wdrożenia oraz dokumentacji powykonawczej do dnia 15 grudnia 2007 r. za cenę netto .....PLN plus podatek VAT w kwocie ..... co daje cenę brutto ..... PLN (słownie: .....).

Łącznie oferujemy wykonanie całości przedmiotu zamówienia za cenę netto .....PLN plus podatek VAT w kwocie ..... co daje cenę brutto ..... PLN (słownie: .....).

Cena zawiera wszelkie koszty, jakie poniesiemy z tytułu realizacji niniejszego zamówienia

Opis oferowanego przedmiotu zamówienia stanowi załącznik do niniejszej oferty.

Termin gwarancji wynosi: ..... od daty podpisania protokołu dostawy.

OŚWIADCZAMY, ŻE :

1. specyfikację istotnych warunków zamówienia otrzymaliśmy od Zamawiającego, zapoznaliśmy się z jej treścią i akceptujemy przed złożeniem niniejszej oferty,
2. niniejsza oferta w pełni spełnia wymagania specyfikacji istotnych warunków zamówienia,
3. pozostajemy związani niniejszą ofertą przez 60 dni licząc od dnia, w którym upłynął terminu składania ofert,
4. w przypadku wybrania naszej oferty zobowiązujemy się zawrzeć z Zamawiającym umowę w/g wzoru otrzymanego wraz ze specyfikacją istotnych warunków zamówienia. Umowę zobowiązujemy się zawrzeć w miejscu i terminie jakie zostaną wskazane przez Zamawiającego,

....., dnia ....

pieczęć i podpis Wykonawcy

Podpisy i pieczątki imienne osób upełnomocnionych do reprezentowania Wykonawcy zgodnie z zapisami w dokumencie stwierdzającym status prawny Wykonawcy (odpisie z właściwego rejestru lub zaświadczeniu o wpisie do ewidencji działalności gospodarczej).

Załącznik nr 2 do specyfikacji istotnych warunków zamówienia w postępowaniu o zamówienie publiczne na modernizację węzła centralnego sieci rozległej IPN

Tabela 1 – Przełącznik rdzeniowy – szt. 2

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
1.	Budowa modularna	**TAK**	
2.	Obudowa przeznaczona do montażu w szafie rack 19'' wyposażona w wentylator	**TAK**	
3.	Redundantne zasilacze o mocy wystarczającej do obsługi urządzenia (wykorzystanie procentowe mocy nie większe niż 30%)	**TAK**	
4.	Łączne pasmo przełącznika	**Min. 700 Gbps**	
5.	Pasmo dostępne na każdy moduł	**Min. 40 Gbps**	
6.	Możliwie szeroka gama dostępnych w ofercie modułów sieciowych i usługowych - co najmniej dostępne: - interfejsy Ethernet (10, 10/100, 10/100/1000, GE, 10GE) - moduły interfejsów szeregowych (co najmniej 8 interfejsów na moduł, dostępne interfejsy V.35, RS449, X.21) - moduły ATM (interfejsy E3, OC-3) - moduły PoS (packet over sonet)	**TAK**	
7.	Liczba portów GE o zmiennej konfiguracji interfejsów	**Min. 8**	

8.	Liczba portów 10/100	**Min. 144**	
9.	Liczba portów 10/100/1000 GE	**Min. 48**	
10.	Przełącznik musi być wyposażony w kartę umożliwiającą zaawansowaną analizę ruchu: - analiza w czasie rzeczywistym - karta wyposażona w 512 MB pamięci RAM - monitorowanie wydajności - monitoring QoS - możliwość przeglądania przechwyconych pakietów	**TAK**	
11.	Możliwość instalacji w przełączniku modułu firewall, IDS oraz kontrolera środowiska WLAN	**TAK**	
12.	Możliwość zarządzania ruchem (QoS – klasyfikacja ruchu na podstawie rozpoznawania aplikacji, adresów, portów, oznaczeń TOS, IP Precedence, DSCP itp., kolejkowanie, statyczne i dynamiczne ograniczanie pasma)	**TAK**	
13.	Zarządzanie przez Telnet, konsolę szeregową, SNMP, SSH	**TAK**	
14.	Możliwość rozbudowy konfiguracji – liczba wolnych slotów na moduły	**Min. 2**	
15.	Liczba interfejsów 1000BaseSX	**8**	
16.	Możliwość zmiany konfiguracji „w locie”, bez konieczności restartu urządzenia (dotyczy dowolnych zmian konfiguracji)	**TAK**	
17.	Możliwość zapisu konfiguracji w pliku tekstowym i jej importu/eksportu za pomocą protokołu FTP lub TFTP	**TAK**	
18.	Możliwość jednoczesnej instalacji kilku obrazów systemu operacyjnego i programowego wyboru kolejności ich uruchamiania	**TAK**	
19.	Roczna gwarancja świadczona na miejscu instalacji sprzętu.	**TAK**	
20.	Serwis gwarancyjny powinien być oparty na świadczeniach gwarancyjnych producenta sprzętu, niezależnych od statusu partnerskiego Wykonawcy - wymagane załączenie do oferty odpowiedniego oświadczenia producenta.	**TAK**	
21.	Urządzenie musi być w pełni kompatybilne z dostarczanym oprogramowaniem do zarządzania siecią.	**TAK**	

Tabela 2 – Główna zapora sieciowa – szt. 1

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
1.	Ochrona nieograniczonej liczby użytkowników	**TAK**	
2.	System zabezpieczeń Firewall oparty na technologii *Statefull Inspection* oraz *Application Level Gateway*	**TAK**	
3.	Możliwość instalacji rozwiązania w architekturze rozproszonej lub zcentralizowanej	**TAK**	
4.	Liczba jednocześnie obsługiwanych przez Firewall sesji jest ograniczona jedynie wydajnością platformy sprzętowej. Oprogramowanie zabezpieczeń może zostać zainstalowane na sprzęcie ogólnego przeznaczenia (m.in. serwery o architekturze Intel i Sun SPARC). Producent zabezpieczeń dostarcza odpowiednio przygotowany do tego celu system operacyjny z wbudowaną obsługą algorytmów rutingu dynamicznego	**TAK**	
5.	Dedykowany system operacyjny obsługujący protokoły RIP v1, RIP v2, BGP, OSPF, dla modułów firewall oraz modułu zarządzania	**TAK**	
6.	Zapora sieciowa musi funkcjonować w trybie redundantnym (licencje na dwie zapory o identycznej funkcjonalności)	**TAK**	
7.	Dynamiczna oraz statyczna translacja adresów (reguły generowane automatycznie lub ręcznie)	**TAK**	
8.	Trójwarstwowa architektura - moduł zabezpieczeń, moduł zarządzania oraz interfejs GUI. Komunikacja pomiędzy modułem zabezpieczeń i modułem zarządzania jest szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych	**TAK**	

9.	Uwierzytelnianie administratorów zapory sieciowej odbywa się za pomocą haseł statycznych, haseł dynamicznych lub certyfikatów cyfrowych. Istnieje możliwość definiowania szczegółowych uprawnień administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników).	**TAK**	
10.	Automatyczne przydzielanie adresów zdalnym użytkownikom	**TAK**	
11.	Polityka bezpieczeństwa Firewall w zakresie kontroli ruchu sieciowego uwzględnia kierunek przepływu pakietów, protokoły i usługi sieciowe, użytkowników i serwery usług, stan połączenia oraz dane aplikacyjne (m.in. obsługuje fragmentację IP, ochronę systemu operacyjnego przed atakami Exploit i DoS)	**TAK**	
12.	Firewall umożliwia identyfikowanie niedozwolonych lub podejrzanych działań, prób ataku oraz po ich wykryciu podnosi alarm (m.in. wykrywa skanowanie portów, IP Spoofing, SYN Flood, CodRad, Nimda).	**TAK**	
13.	Firewall bez dodatkowych aplikacji umożliwia szczegółową kontrolę aplikacji sieciowych (kontroluje rozmiar przesyłek pocztowych, blokuje Mail Relaying, blokuje niedozwolone pliki przesyłane jako załączniki do poczty)	**TAK**	
14.	System zabezpieczeń zawiera wbudowany system wykrywania i ochrony przed intruzami (IPS). Sygnatury ataków są regularnie dostarczane przez producenta zabezpieczeń	**TAK**	
15.	Firewall posiada wiele metod uwierzytelniania użytkowników lokalnych i zdalnych (np. uwierzytelnianie przezroczyste gdzie Firewall przechwytuje sesję i uwierzytelnia jej użytkownika, uwierzytelnianie za pomocą agenta na stacji użytkownika, uwierzytelniania po połączeniu się z modułem Firewall). Baza użytkowników jest przechowywana lokalnie na Firewall lub na zewnętrznym serwerze (np. LDAP)	**TAK**	
16.	Funkcjonalność zabezpieczeń Firewall w razie potrzeby może zostać rozszerzona z użyciem rozwiązań innych dostawców (np. oprogramowanie antywirusowe, urzędy certyfikacji, systemy uwierzytelniania). Integracja Firewall z zabezpieczeniami innych dostawców odbywa się za pomocą dedykowanych protokołów	**TAK**	
17.	Wbudowany wewnętrzny urząd certyfikacji	**TAK**	
18.	Zabezpieczenie danych w sieci VPN odbywa się z użyciem mocnych algorytmów kryptograficznych (m.in. AES-256 i 3DES)	**TAK**	
19.	Rozwiązanie umożliwia dostęp zdalny dla co najmniej 25 użytkowników z wykorzystaniem protokołu IPSEC	**TAK**	
20.	Zarządzanie modułami firewall funkcjonujących w różnych miejscach sieci odbywa się z centralnej, graficznej konsoli administratora GUI. Konsola zarządzania posiada możliwości automatycznej weryfikacji spójności i niesprzeczności wprowadzonej polityki bezpieczeństwa.	**TAK**	
21.	Umożliwia tworzenie sieci VPN w oparciu o standard IPSec/IKE, funkcjonujące w trybie site-site oraz client-site (). Funkcjonalność klienta VPN może zostać rozszerzona o zarządzany centralnie Personal Firewall	**TAK**	
22.	System zabezpieczeń posiada zintegrowany moduł zarządzania pasmem sieci (QoS). Polityka zarządzania pasmem jest definiowana z graficznego interfejsu GUI i uwzględnia priorytety, pasma dopuszczalne i pasma gwarantowane. Administrator za pomocą graficznych narzędzi może obserwować aktualną zajętość pasma sieci przez poszczególnych	**TAK**	

	użytkowników i aplikacje		
23.	Konsola zarządzania zabezpieczeń umożliwia tworzenie raportów graficznych i tekstowych z pracy zabezpieczeń na podstawie rejestrowanych zdarzeń (logów).	**TAK**	
24.	Konsola zarządzania zabezpieczeń umożliwia graficzną prezentację i analizę struktury sieci chronionych. Mapa sieci tworzona jest automatycznie na podstawie definicji obiektów	**TAK**	
25.	Konsola zarządzania zabezpieczeń umożliwia centralą aktualizację oprogramowania zabezpieczeń (m.in. instalację poprawek i nowych wersji)	**TAK**	
26.	Konsola zarządzania zabezpieczeń umożliwia w czasie rzeczywistym obserwację stanu zajętości pasma sieci	**TAK**	
27.	Pomoc techniczna oraz szkolenia z produktu są dostępne w Polsce. Usługi te świadczone są w języku polskim	**TAK**	
Specyfikacja techniczna platformy sprzętowej:			
28.	Maksymalnie 2U do instalacji w standardowej szafie RACK 19”	**TAK**	
29.	Płyta główna z możliwością zainstalowania do dwóch procesorów, szyna FSB do 1333 MHz. Płyta główna musi być produkowana przez producenta serwera i oznaczona jego znakiem firmowym	**TAK**	
30.	Chipset dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych	**TAK**	
31.	Dwa procesory dwurdzeniowe klasy x86 dedykowane do pracy w serwerach zaprojektowane do pracy w układach dwuprocesorowych, taktowane zegarem co najmniej 2.66GHz, częstotliwość szyny systemowej 1333MHz pamięć L2 4 MB lub procesor równoważny wydajnościowo według wyniku testów przeprowadzonych przez Oferenta. W przypadku zaoferowania procesora równoważnego Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzenia testów oferent musi dostarczyć zamawiającemu oprogramowanie testujące, oba równoważne porównywalne zestawy oraz dokładny opis użytych testów wraz z wynikami w celu ich sprawdzenia w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od zamawiającego.	**TAK**	
32.	4 GB DDR2 SDRAM 667MHz FBD, możliwa rozbudowa do 32GB	**TAK**	
33.	Zabezpieczenie pamięci RAM ECC, Chipkill (lub równoważny), spare bank memory, memory mirror	**TAK**	
34.	Minimum 2 x PCI-Express x8 i 1 x PCI-Express x4, z czego min. 2 gniazda umożliwiają instalowanie pełnowymiarowych kart rozszerzeń	**TAK**	
35.	Ilość interfejsów sieciowych 10/100/1000	**Min. 6**	
36.	Wewnętrzny napęd DVD-ROM	**TAK**	

37.	Zainstalowane 2 x 146GB 15krpm typu HotPlug SAS 3.5“	**TAK**	
38.	Zintegrowany kontroler RAID. Pamięć podręczna minimum 256MB, z podtrzymaniem bateryjnym.	**TAK**	
39.	Zintegrowana karta graficzna, pamięć 16 MB	**TAK**	
40.	Wentylatory i zasilacze zapewniające nadmiarowość	**TAK**	
41.	Serwer musi posiadać certyfikat dla: Windows 2003; RedHat Enterprise Linux ES 4.0	**TAK**	
42.	Trzy letnia gwarancja świadczona w miejscu instalacji sprzętu	**TAK**	
43.	Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta serwera – dokumenty potwierdzające załączyć do oferty.	**TAK**	
44.	Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.	**TAK**	
45.	Zamawiający wymaga dokumentacji w języku polskim lub angielskim	**TAK**	
46.	Platforma sprzętowa musi znajdować się na listach kompatybilności producenta oferowanego rozwiązania firewall	**TAK**	

Tabela 3 – Sonda IPS – szt. 1

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
1.	System zabezpieczeń powinien identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), nawiązywanie połączeń Backdoor, ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów	**TAK**	
2.	System zabezpieczeń na bieżąco zbiera i automatycznie aktualizuje informacje na temat występujących w sieciach chronionych komputerów oraz zainstalowanych na nich aplikacjach. Nie są do tego celu wykorzystywane techniki skanowania, a jedynie przezroczysta analiza ruchu sieciowego. System zabezpieczeń pobiera i poddaje korelacji informacje z wielu, występujących różnych segmentach sieci sensorów IPS	**TAK**	
3.	System zabezpieczeń podnosi alarm w razie zauważenia nowych komputerów bądź aplikacji w sieciach chronionych. Administrator zabezpieczeń za pomocą dedykowanych graficznych narzędzi może sprawdzić jakie zmiany wystąpiły w sieci w określonych okresie czasu (m.in. nowe komputery, nowe aplikacje i otwarte porty)	**TAK**	
4.	Administrator zabezpieczeń ma możliwość zdefiniowania zasad normalnej pracy systemu informatycznego i otrzymywać alarmy o naruszeniach przyjętej polityki bezpieczeństwa firmy (m.in. wykorzystywanie przez określonych pracowników niedozwolonych aplikacji)	**TAK**	
5.	Administrator zabezpieczeń może bez konieczności skanowania sieci dowiedzieć się jakie wersje aplikacji serwerów i stacji roboczych znajdują się w sieciach chronionych. Na tej podstawie może wykonać analizę podatności systemu informatycznego na znane błędy bezpieczeństwa oraz w razie zauważenia ataku zweryfikować, czy atakowany system jest	**TAK**	

	na to zagrożenie podatny.		
6.	System zabezpieczeń powinien działać w trybie In-line (tzn. ruch sieciowy przepływa przez urządzenie) oraz Sniffer (tzn. urządzenie zabezpieczeń nasłuchuje ruch sieciowy). W trybie In-line urządzenie może pracować w warstwie 2 i 3 OSI. Tryb pracy zabezpieczeń ustala się w konfiguracji	**TAK**	
7.	System zabezpieczeń dostarczany jest jako dedykowane urządzenie typu Appliance, wyposażone w co najmniej 10 portów 10/100/1000 Ethernet. Urządzenie obsługuje sieci wirtualne VLAN (802.1Q Tagging). Przepływność urządzenia w trybie In-line określona przez producenta nie może być niższa od 240 Mb/s	**TAK**	
8.	Urządzenie zabezpieczeń może zostać podzielone na wirtualne moduły IPS, które poddają kontroli w trybie In-line wiele oddzielnych segmentów sieci (np. sieć LAN i DMZ). W urządzeniu nie ma możliwości komunikacji pomiędzy wirtualnymi modułami IPS	**TAK**	
9.	Trójwarstwowa architektura systemu zabezpieczeń - sensory, serwer zarządzania, interfejs GUI. Serwer zarządzania przechowuje bazę polityk bezpieczeństwa oraz logi. Całość zarządzania IPS oraz obsługa logów odbywa się na serwerze zarządzania. Polityki bezpieczeństwa są tworzone na centralnym serwerze zarządzania i instalowane na sensory IPS w sieci	**TAK**	
10.	Polityka bezpieczeństwa IPS składa się ze zbioru reguł jednoznacznie określających chronione zasoby systemu informatycznego, rodzaje i źródła zagrożenia oraz reakcję zabezpieczeń na te zagrożenia. Definiowanie reguł odbywa się za pomocą graficznego edytora polityki bezpieczeństwa (nie dopuszcza się zarządzania zabezpieczeń przez przeglądarkę Web). Reguły polityki bezpieczeństwa automatycznie instalują odpowiednie sygnatury ataków na sensorach IPS	**TAK**	
11.	Aktualizacja bazy sygnatur ataków odbywa się co najmniej raz w tygodniu w trybie on-line. Nowe sygnatury po akceptacji administratora są automatycznie aktywowane w odpowiednich regułach polityki bezpieczeństwa	**TAK**	
12.	Administratorzy mogą za pomocą graficznego edytora definiować własne sygnatury ataków i innych zdarzeń	**TAK**	
13.	Produkt wykorzystuje co najmniej trzy różne techniki identyfikowania ataków (np. sygnatury ataków, anomalie protokołów, wykrywanie ataków DoS)	**TAK**	
14.	System zabezpieczeń powinien posiadać mechanizmy ochrony przed zagrożeniami związanymi z wykorzystywaniem internetowych aplikacji współdzielenia zasobów i komunikacji P2P (Peer-to-Peer). Wykrywanie aplikacji P2P odbywa się na dowolnych portach	**TAK**	
15.	System zabezpieczeń IPS powinien analizować ruch sieciowych za pomocą technik heurystycznych (tzn. nie za pomocą sygnatur) np. w celu identyfikowania połączeń Backdoor lub ataków DoS	**TAK**	

16.	System zabezpieczeń IPS posiada szeroki zakres reakcji na zdarzenia (dostępne są co najmniej opcje zablokowania połączenia lub pakietu, reset sesji TCP, zarejestrowanie zdarzenia w logu, zapisanie w logu całości sesji, przesłanie danych do serwera Syslog, powiadomienia poprzez E-Mail i SNMP, zablokowanie ruchu z komputera wykonującego atak na określony czas). Administratorzy mają możliwość definiowania własnych reakcji	**TAK**	
17.	System zabezpieczeń IPS umożliwia rejestrowanie całości komunikacji z komputera, z którego został zidentyfikowany atak (tzn. określonej liczby pakietów przed i po wystąpieniu ataku)	**TAK**	
18.	Konsola zabezpieczeń zawiera graficzne narzędzia umożliwiające przeglądanie zawartości pakietów, w których zidentyfikowane zostały ataki. IPS umożliwia rejestrowanie określonej liczby pakietów przed oraz po wystąpieniu ataku w celu dokładnej analizy całości zdarzenia. Oprócz narzędzi dostępnych w konsoli IPS zarejestrowany ruch może być także przeglądany i analizowany za pomocą innych dostępnych narzędzi (np. Ethereal)	**TAK**	
19.	System zabezpieczeń w momencie zidentyfikowania ataku może blokować odpowiednie pakiety, całkowicie izolując atak od chronionych zasobów systemu informatycznego	**TAK**	
20.	Administratorzy zabezpieczeń mają do dyspozycji zestaw narzędzi wspomagający ich w zarządzaniu bezpieczeństwem. Korelacja i analiza rejestrowanych zdarzeń oraz prezentacja informacji o wykrywanych naruszeniach bezpieczeństwa odbywa się w czasie rzeczywistym. Konsola zarządzająca w formie graficznej prezentuje tworzone w czasie rzeczywistym zestawienia i statystyki (m.in. najczęściej wykonywane ataki, najczęstsze źródła ataków, najczęstsze cele ataków)	**TAK**	
21.	Konsola zabezpieczeń posiada możliwość prezentowania graficznych raportów z pracy zabezpieczeń. Administratorzy mają do dyspozycji predefiniowane raporty. W razie potrzeby mogą definiować własne raporty bez konieczności zakupu dodatkowych licencji	**TAK**	
22.	Pomoc techniczna oraz szkolenia z produktu są dostępne w Polsce. Usługi te świadczone są w języku polskim.	**TAK**	

Tabela 4 – System antywirusowy – szt. 1

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
1.	ilość wymaganych licencji	**2000**	
2.	Możliwość instalacji na systemach Windows 2000/2003 Server , Windows 2003 64 bit	**TAK**	
3.	Usuwanie niepożądanych treści typu „wirus”, „trojan”, „dialer”, „worm”, „exploit”, „spam” przesyłanych przy pomocy protokołów SMTP, HTTP oraz FTP over http	**TAK**	
4.	Wsparcie autentykacji „POP3 before SMTP” oraz protokołu SNMP	**TAK**	
5.	Możliwość pracy w trybie chained-proxy, parent proxy, reverse-proxy	**TAK**	
6.	Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie przesyłane dane	**TAK**	
7.	aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie	**TAK**	
8.	aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym	**TAK**	
9.	brak konieczności ponownego uruchomienia serwera po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów	**TAK**	

10.	heurystyczna technologia do wykrywania nowych, nieznanych wirusów	**TAK**	
11.	mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona	**TAK**	
12.	mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji)	**TAK**	
13.	obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej : ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2	**TAK**	
14.	automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa	**TAK**	
15.	automatyczne uruchamianie procedur naprawczych	**TAK**	
16.	uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione	**TAK**	
17.	gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin	**TAK**	
18.	średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365)	**TAK**	
19.	Zarządzanie poprzez przeglądarkę WWW oraz centralnie z poziomu jednolitego systemu centralnego zarządzania dla systemów antywirusowych oferowanych przez producenta	**TAK**	
20.	Możliwość zakupu opcji dodatkowej pozwalającej na: • Obsługiwanie serwerów RBL (Real-Time Blackhole) • Możliwość dodawania własnych reguł i klasyfikowania wiadomości jako spam, nie-spam i innych • Możliwość definiowania czarnych i białych list nadawców, odbiorców, domen internetowych, adresów IP, itp	**TAK**	
21.	Możliwość współpracy z innymi produktami antywirusowymi producenta dla serwerów/gateway'ów na tej samej stacji roboczej/serwerze	**TAK**	
22.	Definiowanie własnych powiadomień i ostrzeżeń, także w języku polskim	**TAK**	
23.	Kwarantanna lokalna dla treści sklasyfikowanych jako niebezpieczne	**TAK**	
24.	Możliwość usuwania tylko i wyłącznie niebezpiecznych elementów (np. załącznik w przesyłce e-mail lub skrypt Active-X) z analizowanych danych	**TAK**	
25.	Wykrywanie treści zaszyfrowanych i zahasłowanych z możliwością traktowania ich jako niebezpieczne	**TAK**	

26.	inteligentne rozpoznawanie plików i załączników, niezależnie od tego jakie rozszerzenie one posiadają	**TAK**	
27.	Możliwość instalacji konsoli centralnego zarządzania, serwera centralnego zarzadzania, serwera automatycznego raportowania oraz wewnętrznego serwera aktualizacji (proxy) na systemie Windows 2000/2003 Server oraz Linux	**TAK**	
28.	Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) oraz JAR	**TAK**	
29.	Możliwość wykonania bezpośredniej instalacji zdalnej nienadzorowanej	**TAK**	
30.	narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nowe wersję	**TAK**	
31.	pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem)	**TAK**	
32.	komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi	**TAK**	
33.	pełne centralne zarządzanie dla środowisk Windows 98, Windows ME, Windows NT Server & Workstation, Windows 2000, Windows 2003, Windows XP, Linux	**TAK**	
34.	scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta	**TAK**	
35.	administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa	**TAK**	
36.	centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy	**TAK**	
37.	możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów)	**TAK**	
38.	tworzenie grup , zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach	**TAK**	
39.	możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych i w celu uniemożliwienia ich modyfikacji przez użytkowników	**TAK**	
40.	możliwość wyłączenia blokady zmiany ustawień dla użytkownika z prawami administratora	**TAK**	
41.	serwer zarządzający związany z konsolą zarządzającą musi mieć funkcję przesyłania aktualizacji do klientów z możliwością ustawienia harmonogramu lub częstotliwości aktualizacji	**TAK**	
42.	możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający	**TAK**	

43.	możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji	**TAK**	
44.	możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta	**TAK**	
45.	funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania	**TAK**	
46.	dane powinny być przesyłane do serwera zarządzania podczas kolejnego połączenia	**TAK**	
47.	możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich	**TAK**	
48.	program musi pozwalać administratorowi zdefiniować treść komunikatu wyświetlanego w przypadku wykrycia wirusa	**TAK**	
49.	umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe	**TAK**	
50.	automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji	**TAK**	
51.	automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej niż co 7 dni (zalecane codzienne aktualizacje)	**TAK**	
52.	automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe	**TAK**	
53.	możliwość automatycznego raportowania do pliku w formacie HTML i CSV	**TAK**	
54.	możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich	**TAK**	
55.	możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”	**TAK**	
56.	możliwość lokalnego zarządzania wszystkimi ustawieniami programu klienta	**TAK**	
57.	program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa	**TAK**	
58.	program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe	**TAK**	
59.	program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy)	**TAK**	

60.	program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów	**TAK**	
61.	zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna, powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania	**TAK**	

Tabela 5 – Oprogramowanie do zarządzania siecią – szt. 1

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
Oprogramowanie do zarządzania siecią LAN			
1.	Możliwość zarządzania co najmniej 300 urządzeniami	**TAK**	
2.	Umożliwia tworzenie, usuwanie i edycję VLANów	**TAK**	
3.	Automatyczne wykrywanie powszechnych problemów w sieci bez konieczności wprowadzania definicji przez użytkowników	**TAK**	
4.	Możliwość zarządzania w warstwie 2 oraz 3 modelu ISO/OSI	**TAK**	
5.	Możliwość przeglądania informacji dotyczących urządzeń sieciowych: pamięć, gniazda, wersje oprogramowania	**TAK**	
6.	Możliwość wysłania aktualizacji oprogramowania i konfiguracji do wybranych urządzeń w sieci	**TAK**	
7.	Monitoring użytkowników i aplikacji aktywnych w sieci	**TAK**	
8.	Wymagania systemowe dla serwera: Windows 2000 Professional, Server i Advanced Server z Service Pack 4, Windows Server 2003 Standard i Enterprise Editions z Service Pack 1, Windows 2003 R2 Server Standard i Enterprise Editions, Solaris 8, Solaris 9	**TAK**	
9.	Wymagania systemowe dla klienta: Windows 2000 Professional, Server i Advanced Server z Service Pack 4, Windows Server 2003 Standard i Enterprise Edition z Service Pack 1, Windows 2003 R2 Server Standard i Enterprise Editions,	**TAK**	

	Windows XP z Service Pack 2, Solaris 8, Solaris 9, przeglądarka internetowa: Internet Explorer 6.0, Netscape Navigator 7.0, 7.1 i 7.2, Mozilla 1.7.13		
10.	Oprogramowanie musi być w pełni kompatybilne z sieciowymi urządzeniami aktywnymi Zamawiającego	**TAK**	
Oprogramowanie do zarządzania polityką jakości ruchu			
1.	Możliwość obsługi nieograniczonej liczby urządzeń	**TAK**	
2.	Centralne zarządzanie tworzeniem polityk, weryfikacją, wdrożeniem oraz monitoringiem	**TAK**	
3.	możliwość dzielenia sieć na domeny oraz używania polityk do konfigurowania globalnych ustawień QoS	**TAK**	
4.	zarządzanie przez przeglądarkę internetową	**TAK**	
5.	możliwość tworzenia polityki QoS za pomocą kreatora	**TAK**	
6.	możliwość zarządzania przeciążeniem, unikania przeciążeń oraz kontroli przepustowości przez wybiórcze aktywowanie mechanizmów QoS w pogrupowanych interfejsach LAN i WAN	**TAK**	
7.	możliwość wykrywania konfliktów polityki QoS, instalowania istniejącej konfiguracji urządzeń, definiowania zasięgu list kontroli dostępu oraz odtwarzania poprzedniej wersji polityki	**TAK**	
8.	Wymagania systemowe dla serwera: Windows 2000 Professional, Server i Advanced Server (z Service Pack 3 lub 4) lub Windows Serwer 2003	**TAK**	
9.	Wymagania systemowe dla klienta: Windows 2000 (Server lub Professional Edition) z Service Pack 3 lub 4, lub Windows XP SP1 (Server i Professional), przeglądarka internetowa Microsoft Internet Explorer 6.0 lub Netscape Navigator 7.1	**TAK**	
10.	Oprogramowanie musi być w pełni kompatybilne z sieciowymi urządzeniami aktywnymi Zamawiającego	**TAK**	
Oprogramowanie do zarządzania bezpieczeństwem urządzeń			
1.	Możliwość scentralizowanego zarządzania nieograniczonej liczby zapór sieciowych oraz systematów IPS/IDS	**TAK**	
2.	Możliwość konfiguracji wspólnych zasad, które można globalnie wdrażać dla wszystkich urządzeń	**TAK**	
3.	Możliwość cyklicznych i automatycznych aktualizacji oprogramowania i konfiguracji firewall-i	**TAK**	

4.	Możliwość konfiguracji sond za pomocą profili grup	**TAK**	
5.	Możliwość konfiguracji i zarządzanie połączeniami VPN	**TAK**	
6.	Możliwość konfiguracji protokołu IPSec w sieciach VPN	**TAK**	
7.	Oprogramowanie powinno korelować zdarzenia w celu zidentyfikowania ataku, który nie był by widoczny poprzez pojedyncze zdarzenie	**TAK**	
8.	Wymagania systemowe dla serwera: Windows 2000 Professional, Server i Advanced Server (Service Pack 4) lub Windows Server 2003	**TAK**	
9.	Wymagania systemowe dla klienta: Windows 2000 Server, Professional Edition z Service Pack 4 lub Windows XP z Service Pack 2, przeglądarka internetowa Internet Explorer 6 lub Netscape Navigator 7.1	**TAK**	
10.	Oprogramowanie musi być w pełni kompatybilne z sieciowymi urządzeniami aktywnymi Zamawiającego	**TAK**	
Oprogramowanie do zarządzania konfiguracją urządzeń			
1.	Możliwosc zarządzania co najmniej 100 urządzeniami	**TAK**	
2.	Możliwość śledzenia wszystkich zmian w konfiguracji, oprogramowaniu i sprzęcie sieciowym	**TAK**	
3.	Wyświetlanie wszystkich zmian w polityce firmy oraz natychmiastowe sprawdzanie zgodności	**TAK**	
4.	Automatyczna weryfikacja wprowadzanych zmian konfiguracyjnych	**TAK**	
5.	Możliwość definicji praw administratorów	**TAK**	
6.	Możliwość wymuszania przez administratorów zastosowania określonej konfiguracji	**TAK**	
7.	Monitorowanie nieautoryzowanych i nieplanowanych zmian	**TAK**	
8.	Umożliwia zarządzanie konfiguracją: routerów, firewalli, punktów dostępowych sieci bezprzewodowej oraz urządzeń VPN	**TAK**	
9.	Wymagania systemowe: Windows Server 2000, 2003 Enterprise Edition, Solaris 9 lub 10, RedHat Linux AS 3.0 Update 2 lub AS 4.0, Suse Linux Enterprise Server 9, baza danych: MySQL Max 3.23	**TAK**	

10.	Oprogramowanie musi być w pełni kompatybilne z sieciowymi urządzeniami aktywnymi Zamawiającego	**TAK**	

Tabela 6 – Router centralny WAN – szt. 1

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
1.	urządzenie modularne	**TAK**	
2.	możliwość instalacji redundantnych zasilaczy	**TAK**	
3.	wydajność routowania min. 500 kpps (dla pakietów 64B)	**TAK**	
4.	możliwie szeroka gama dostępnych w ofercie modułów sieciowych i usługowych - co najmniej dostępne: – moduły interfejsów szeregowych (interfejsy V.35, RS449, X.21) – moduły ATM (interfejsy E3) moduły Ethernet, FastEthernet i GigabitEthernet	**TAK**	
5.	zainstalowany moduł z dwoma portami szeregowym (wymagane dołączenie okablowania dla styków V.35)	**TAK**	
6.	zainstalowany moduł analizatora sieciowego, do zaawansowanej inspekcji ruchu	**TAK**	
7.	co najmniej dwa porty GE (10/100/1000)	**TAK**	
8.	wsparcie dla protokołów routingu BGP, OSPF i EIGRP	**TAK**	

9.	wsparcie dla protokołu MPLS	**TAK**	
10.	możliwość zestawiania tuneli IPSec VPN z szyfrowaniem 3DES i AES – wydajność szyfrowania min. 200 Mbps (dla pakietów 1400B)	**TAK**	
11.	możliwość autoryzacji tuneli VPN za pomocą współdzielonych haseł, certyfikatów cyfrowych X.509, serwera autoryzacyjnego, protokołów PAP/CHAP	**TAK**	
12.	możliwość zarządzania ruchem (QoS – klasyfikacja ruchu na podstawie rozpoznawania aplikacji, adresów, portów, oznaczeń TOS, IP Precedence, DSCP itp., kolejkowanie, statyczne i dynamiczne ograniczanie pasma)	**TAK**	
13.	możliwość instalacji modułów VoIP i obsługi połączeń głosowych	**TAK**	
14.	możliwość instalacji modułów IDS	**TAK**	
15.	zarządzanie przez Telnet, konsolę szeregową, SNMP, SSH, dedykowaną aplikację	**TAK**	
16.	możliwość zmiany konfiguracji „w locie", bez konieczności restartu urządzenia (dotyczy dowolnych zmian konfiguracji)	**TAK**	
17.	możliwość zapisu konfiguracji w pliku tekstowym i jej importu/eksportu za pomocą protokołu FTP lub TFTP	**TAK**	
18.	możliwość jednoczesnej instalacji kilku obrazów systemu operacyjnego i programowego wyboru kolejności ich uruchamiania	**TAK**	
19.	roczna gwarancja świadczona na miejscu instalacji sprzętu.	**TAK**	
20.	serwis gwarancyjny powinien być oparty na świadczeniach gwarancyjnych producenta sprzętu, niezależnych od statusu partnerskiego Wykonawcy - wymagane załączenie do oferty odpowiedniego oświadczenia producenta.	**TAK**	
21.	urządzenie musi być w pełni kompatybilne z posiadanym przez Zamawiającego oprogramowaniem do zarządzania siecią.	**TAK**	

Tabela 7 – Routery oddziałowe typ I – szt. 13

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
1.	urządzenie modularne	**TAK**	
2.	możliwość instalacji redundantnych zasilaczy	**TAK**	
3.	wydajność routowania min. 160 kpps (dla pakietów 64B)	**TAK**	
4.	możliwie szeroka gama dostępnych w ofercie modułów sieciowych i usługowych - co najmniej dostępne: – moduły interfejsów szeregowych (interfejsy V.35, RS449, X.21) – moduły ATM (interfejsy E3) – moduły Ethernet, FastEthernet i GigabitEthernet	**TAK**	
5.	co najmniej dwa interfejsy Gigabit Ethernet 10/100/1000 dla realizacji połaczenia do sieci LAN	**TAK**	
6.	zainstalowany moduł z portem szeregowym (wymagane dołączenie okablowania dla styków V.35)	**TAK**	
7.	zainstalowany moduł analizatora sieciowego, do zaawansowanej inspekcji ruchu	**TAK**	
8.	minimum 2 porty USB	**TAK**	

9.	minimum dwa porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu	**TAK**	
10.	co najmniej 64MB pamięci Flash i możliwość jej rozbudowy do minimum 256MB	**TAK**	
11.	co najmniej 256MB pamięci DRAM i możliwość jej rozbudowy do minimum 1024MB	**TAK**	
12.	możliwość routingu pakietów zgodnie z protokołami RIP, OSPF, BGP	**TAK**	
13.	obsługa mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2	**TAK**	
14.	wsparcie dla Policy Based Routing (PBR)	**TAK**	
15.	filtrowanie ruchu poprzez zastosowanie list dostępowych (Access List). Filtrowanie powinno być możliwe w oparciu o źródłowe i docelowe adresy IP, źródłowe i docelowe nr portów usługowych, flagi TCP, opcje IP. Filtrowanie powinno być możliwe z ustanowieniem restrykcji czasowych (pora dnia, dni tygodnia)	**TAK**	
16.	obsługa protokółu GRE oraz honorowanie IP Precendence dla ruchu tunelowanego	**TAK**	
17.	wsparcie dla protokołów WCCP i WCCPv2	**TAK**	
18.	Obsługa IPSec NAT Transparency	**TAK**	
19.	obsługa IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode	**TAK**	
20.	funkcjonalność stateful firewall (także dla ICMP) z funkcjami proxy uwierzytelnienia dla ruchu HTTP, FTP i Telnet	**TAK**	
21.	funkcjonalność transparent firewall	**TAK**	
22.	funkcjonalność Network Address Translation (NAT)	**TAK**	
23.	Obsługa IEEE 802.1Q VLAN Trunking	**TAK**	
24.	obsługa mechanizmu DiffServ	**TAK**	
25.	możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu	**TAK**	

26.	obsługa mechanizmu WRED	**TAK**	
27.	zarządzanie przez SNMP, SNMP2c i SNMPv3	**TAK**	
28.	obsługa RMON	**TAK**	
29.	możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS lub TACACS+	**TAK**	
30.	zarządzanie przez Telnet, konsolę szeregową, SNMP, SSH, dedykowaną aplikację	**TAK**	
31.	możliwość zmiany konfiguracji „w locie", bez konieczności restartu urządzenia (dotyczy dowolnych zmian konfiguracji)	**TAK**	
32.	możliwość zapisu konfiguracji w pliku tekstowym i jej importu/eksportu za pomocą protokołu FTP lub TFTP	**TAK**	
33.	możliwość jednoczesnej instalacji kilku obrazów systemu operacyjnego i programowego wyboru kolejności ich uruchamiania	**TAK**	
34.	roczna gwarancja świadczona na miejscu instalacji sprzętu.	**TAK**	
35.	serwis gwarancyjny powinien być oparty na świadczeniach gwarancyjnych producenta sprzętu, niezależnych od statusu partnerskiego Wykonawcy - wymagane załączenie do oferty odpowiedniego oświadczenia producenta.	**TAK**	
36.	urządzenie musi być w pełni kompatybilne z posiadanym przez Zamawiającego oprogramowaniem do zarządzania siecią.	**TAK**	

Tabela 8 – Routery oddziałowe typ II – szt. 9

Producent:
Model/Typ:

Produkt (numer katalogowy)	Opis	Ilość

Lp.	Parametr	Wymagania zamawiającego	Potwierdzenie spełnienia wymagań
1.	urządzenie modularne	**TAK**	
2.	możliwość instalacji redundantnych zasilaczy	**TAK**	
3.	wydajność routowania min. 110 kpps (dla pakietów 64B)	**TAK**	
4.	możliwie szeroka gama dostępnych w ofercie modułów sieciowych i usługowych - co najmniej dostępne: – moduły interfejsów szeregowych (interfejsy V.35, RS449, X.21) – moduły ATM (interfejsy E3) – moduły Ethernet, FastEthernet i GigabitEthernet	**TAK**	
5.	co najmniej dwa interfejsy Gigabit Ethernet 10/100 dla realizacji połączenia do sieci LAN	**TAK**	
6.	zainstalowany moduł z portem szeregowym (wymagane dołączenie okablowania dla styków V.35)	**TAK**	
7.	zainstalowany moduł analizatora sieciowego, do zaawansowanej inspekcji ruchu	**TAK**	
8.	minimum 2 porty USB	**TAK**	

9.	minimum dwa porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu	**TAK**	
10.	co najmniej 64MB pamięci Flash i możliwość jej rozbudowy do minimum 256MB	**TAK**	
11.	co najmniej 256MB pamięci DRAM i możliwość jej rozbudowy do minimum 768MB	**TAK**	
12.	możliwość routingu pakietów zgodnie z protokołami RIP, OSPF, BGP	**TAK**	
13.	obsługa mechanizmów związanych z obsługą ruchu multicast: IGMP v3, IGMP Snooping, PIMv1, PIMv2	**TAK**	
14.	wsparcie dla Policy Based Routing (PBR)	**TAK**	
15.	filtrowanie ruchu poprzez zastosowanie list dostępowych (Access List). Filtrowanie powinno być możliwe w oparciu o źródłowe i docelowe adresy IP, źródłowe i docelowe nr portów usługowych, flagi TCP, opcje IP. Filtrowanie powinno być możliwe z ustanowieniem restrykcji czasowych (pora dnia, dni tygodnia)	**TAK**	
16.	obsługa protokółu GRE oraz honorowanie IP Precendence dla ruchu tunelowanego	**TAK**	
17.	wsparcie dla protokołów WCCP i WCCPv2	**TAK**	
18.	Obsługa IPSec NAT Transparency	**TAK**	
19.	obsługa IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode	**TAK**	
20.	funkcjonalność stateful firewall (także dla ICMP) z funkcjami proxy uwierzytelnienia dla ruchu HTTP, FTP i Telnet	**TAK**	
21.	funkcjonalność transparent firewall	**TAK**	
22.	funkcjonalność Network Address Translation (NAT)	**TAK**	
23.	Obsługa IEEE 802.1Q VLAN Trunking	**TAK**	
24.	obsługa mechanizmu DiffServ	**TAK**	
25.	możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu	**TAK**	

26.	obsługa mechanizmu WRED	**TAK**	
27.	zarządzanie przez SNMP, SNMP2c i SNMPv3	**TAK**	
28.	obsługa RMON	**TAK**	
29.	możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS lub TACACS+	**TAK**	
30.	zarządzanie przez Telnet, konsolę szeregową, SNMP, SSH, dedykowaną aplikację	**TAK**	
31.	możliwość zmiany konfiguracji „w locie", bez konieczności restartu urządzenia (dotyczy dowolnych zmian konfiguracji)	**TAK**	
32.	możliwość zapisu konfiguracji w pliku tekstowym i jej importu/eksportu za pomocą protokołu FTP lub TFTP	**TAK**	
33.	możliwość jednoczesnej instalacji kilku obrazów systemu operacyjnego i programowego wyboru kolejności ich uruchamiania	**TAK**	
34.	roczna gwarancja świadczona na miejscu instalacji sprzętu.	**TAK**	
35.	serwis gwarancyjny powinien być oparty na świadczeniach gwarancyjnych producenta sprzętu, niezależnych od statusu partnerskiego Wykonawcy - wymagane załączenie do oferty odpowiedniego oświadczenia producenta.	**TAK**	
36.	urządzenie musi być w pełni kompatybilne z posiadanym przez Zamawiającego oprogramowaniem do zarządzania siecią.	**TAK**	

Załącznik nr 3 do specyfikacji istotnych warunków zamówienia w postępowaniu o zamówienie publiczne na modernizację węzła centralnego sieci rozległej IPN

Wykaz lokalizacji i miejsc dostawy urządzeń

Załącznik nr 4 do specyfikacji istotnych warunków zamówienia w postępowaniu o zamówienie publiczne na modernizację węzła centralnego sieci rozległej IPN

Wykaz miejsc instalacji, konfiguracji i integracji urządzeń

L.p.	Lokalizacja	Jednostka nadrzędna	Router centralny - tabela 1	Router oddziałowy - tabela 2	Router oddziałowy - tabela 3
1	Centrala IPN ul. Towarowa 28 00-839 Warszawa	Centrala	1 szt.		
2	BEP Warszawa Hrubieszowska 6a 01-209 Warszawa	Centrala		1 szt.	
3	BUiAD Warszawa ul. Kłobucka 21 Warszawa	Centrala		1 szt.	
4	Oddział Warszawa ul. Pl. Krasińskich 2/4/6 00-207 Warszawa	Centrala		1 szt.	
5	Oddział Warszawa ul. Chłodna 51 00-867 Warszawa	Centrala			1 szt.
6	Oddział Białystok ul. Warsztatowa 1a 15-637 Białystok	Oddział Białystok		1 szt.	
7	Oddział Gdańsk ul. Witomińska 19 81-311 Gdynia	Oddział Gdańsk		1 szt.	
8	Oddział Gdańsk ul. Polanki 124 80-308 Gdańsk	Oddział Gdańsk			1 szt.
9	Delegatura Bydgoszcz ul. Grudziądzka 9-15 85-130 Bydgoszcz	Oddział Gdańsk			1 szt.
10	Oddział Katowice ul. Kilińskiego 9 40-061 Katowice	Oddział Katowice		1 szt.	
11	Oddział Katowice ul. Józefowska 102 40-145 Katowice	Oddział Katowice			1 szt.
12	Oddział Kraków ul. Reformacka 3 31-012 Kraków	Oddział Kraków		1 szt.	
13	Oddział Kraków ul. Skulimowskiego 1 Wieliczka	Oddział Kraków			1 szt.
14	Delegatura Kielce Al. Na Stadion 1 25-127 Kielce	Oddział Kraków			1 szt.
15	Oddział Lublin ul. Szewska 2 20-086 Lublin	Oddział Lublin		1 szt.	

L.p.	Lokalizacja	Jednostka nadrzędna	Router centralny - tabela 1	Router oddziałowy - tabela 2	Router oddziałowy - tabela 3
16	Oddział Lublin ul. Wieniawska 15 20-071 Lublin	Oddział Lublin			1 szt.
17	Delegatura Radom ul. Żeromskiego 53 26-600 Radom	Oddział Lublin			1 szt.
18	Oddział Łódź ul. Orzeszkowej 31/35 91-479 Łódź	Oddział Łódź		1 szt.	
19	Oddział Łódź ul. Piotrkowska 149 90-440 Łódź	Oddział Łódź			1 szt.
20	Oddział Poznań ul. Rolna 45a 61-487 Poznań	Oddział Poznań		1 szt.	
21	Oddział Rzeszów ul. Słowackiego 18 35-060 Rzeszów	Oddział Rzeszów		1 szt.	
22	Oddział Szczecin ul. K. Janickiego 30 71-270 Szczecin	Oddział Szczecin		1 szt.	
23	Oddział Wrocław ul. Sołtysowicka 21a 51-168 Wrocław	Oddział Wrocław		1 szt.	

Urządzenia nie wymienione w zestawieniu instalowane będą w siedzibie Instytutu Pamięci Narodowej przy ul. Towarowej 28.

Załącznik nr 5 do specyfikacji istotnych warunków zamówienia w postępowaniu o zamówienie publiczne na modernizację węzła centralnego sieci rozległej IPN

Wzór oświadczenia Wykonawcy o spełnianiu przez niego warunków określonych w art. 22 ust. 1 ustawy dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tekst jednolity: Dz. U. z 2006 r., Nr 163, poz. 1163 ze zm.)

Ja (imię i nazwisko) .....
zamieszkały.....
reprezentując firmę (nazwa firmy).....
.....
jako (stanowisko służbowe) .....
w imieniu swoim i reprezentowanej przeze mnie firmy oświadczam, że:.

1) posiadamy uprawnienia do wykonywania działalności (art. 22 ust. 1 pkt 1),
2) posiadamy niezbędną wiedzę i doświadczenie oraz dysponujemy potencjałem technicznym i osobami zdolnymi do wykonania zamówienia (art. 22 ust. 1 pkt 2),
3) nasza sytuacja finansowa i ekonomiczna zapewni wykonanie wyżej wymienionego zamówienia (art. 22 ust. 1 pkt 3),
4) nie podlegamy wykluczeniu z postępowania o udzielenie zamówienia (art. 22 ust. 1 pkt 4) .

....., dnia ..... 2007 r. .....
pieczęć i podpis Wykonawcy

Podpisy i pieczątki imienne osób upełnomocnionych do reprezentowania Wykonawcy zgodnie z zapisami w dokumencie stwierdzającym status prawny Wykonawcy (odpisie z właściwego rejestru lub zaświadczeniu o wpisie do ewidencji działalności gospodarczej).

Załącznik nr 6 do specyfikacji istotnych warunków zamówienia w postępowaniu o zamówienie publiczne na modernizację węzła centralnego sieci rozległej IPN

UMOWA

W dniu 2007 r. w Warszawie, pomiędzy:

Instytutem Pamięci Narodowej – Komisją Ścigania Zbrodni przeciwko Narodowi Polskiemu z siedzibą w Warszawie przy Pl. Krasińskich 2/4/6, zwanym dalej „Zamawiającym", reprezentowanym przez:

Pana Jana Bastera – Dyrektora Generalnego,

.....
.....,
zwanym dalej „Wykonawcą", reprezentowanym przez:

.....,

została zawarta umowa następującej treści:

§ 1
PODSTAWA ZAWARCIA UMOWY

Na podstawie przeprowadzonego postępowania o zamówienie publiczne w trybie przetargu nieograniczonego, zgodnie z ustawą Prawo zamówień publicznych, Zamawiający zleca a Wykonawca przyjmuje do realizacji przedmiot umowy określony w § 2 umowy.

§ 2
PRZEDMIOT UMOWY

1. Przedmiotem umowy jest modernizacja węzła centralnego sieci rozległej WAN tj. zakup wraz z instalacją, konfiguracją i integracją z infrastrukturą sieciową Zamawiającego następujących fabrycznie nowych nieużywanych urządzeń sieciowych i oprogramowania:
   - modularnych przełączników rdzeniowych - 2 szt,
   - firewalla (główna zapora sieciowa) – 1 szt,
   - systemu antywirusowego – 1 szt,
   - automatycznego systemu analizy i zapobiegania zagrożeń IPS (sonda IPS) – 1 szt,
   - oprogramowania do analizy i zarządzania siecią oraz urządzeniami – 1 szt,
   - routerów z możliwością analizy ruchu oraz zarządzania pasmem: 1 szt. – router centralny, 13 szt. router oddziałowy typ I, 9 szt router oddziałowy typ II,

   szczegółowo opisanych w ofercie, stanowiącej załącznik nr 1 do umowy.
2. Wykonawca dostarczy urządzenia i oprogramowanie o których mowa w ust. 1 do lokalizacji, określonych w załączniku nr 2 do umowy „Wykaz lokalizacji i miejsc dostawy urządzeń" i następnie dokona ich instalacji, konfiguracji i integracji zgodnie z załącznikiem nr 3 do umowy „Wykaz miejsc instalacji, konfiguracji i integracji urządzeń" na zasadach określonych w załączniku nr 4 do umowy „Instalacja, konfiguracja oraz integracja z istniejącą infrastrukturą teleinformatyczną".

§ 3
TERMIN REALIZACJI

1. Realizacja przedmiotu umowy nastąpi w II etapach:
   I etap – dostawa urządzeń sieciowych i oprogramowania - w ciągu 45 dni od daty zawarcia umowy,
   II etap – opracowanie projektu wdrożenia – instalacji, konfiguracji i integracji, uzgodnienie dokumentu projektowego z zamawiającym, wykonanie wdrożenia oraz dokumentacji powykonawczej do dnia 15 grudnia 2007 r.

2. W celu potwierdzenia realizacji przedmiotu umowy Wykonawca zobowiązany jest przedstawić Zamawiającemu kompletnie wypełnione i podpisane protokoły dostawy /usługi.

§ 4
WYNAGRODZENIE WYKONAWCY

1. Za realizację przedmiotu umowy określonego w § 2, Zamawiający zobowiązuje się zapłacić Wykonawcy wynagrodzenie w dwóch częściach, po wykonaniu każdego etapu określonego w § 3 umowy, to znaczy :

I etapu – wynagrodzenie ..... netto PLN plus podatek VAT w kwocie.....
co daje **wartość brutto** ..... PLN (słownie.....
..... PLN brutto),
II etapu – wynagrodzenie ..... netto PLN plus podatek VAT w kwocie.....
co daje **wartość brutto** ..... PLN (słownie.....
..... PLN brutto),
co daje łączne wynagrodzenie za realizację przedmiotu umowy w wysokości .....
netto PLN plus podatek VAT w kwocie..... co
daje **wartość brutto** ..... PLN (słownie.....PLN
brutto).

2. Wynagrodzenie wymienione w ust. l obejmuje wszelkie koszty jakie poniesie Wykonawca z tytułu należytej i zgodnej z niniejszą umową oraz obowiązującymi przepisami realizacji przedmiotu umowy, w tym w szczególności cenę dostarczonych urządzeń i oprogramowania wraz z instalacją, konfiguracją i integracją, koszty transportu, ubezpieczenia, rozładunku oraz wszelkie koszty jakie poniesie Wykonawca z tytułu realizacji przedmiotu umowy.
3. Płatność zostanie uruchomiona po zatwierdzeniu protokołów dostawy/usługi przez Zamawiającego.

§5
WARUNKI DOSTAWY/USŁUGI

1. Ze strony Zamawiającego osobą uprawnioną do kontaktów z Wykonawcą w sprawach dotyczących realizacji przedmiotu umowy jest Pan Krzysztof Lenart, tel. (22) 581-88-99.
2. Ze strony Wykonawcy osobą uprawnioną do kontaktów z Zamawiającym w sprawach dotyczących realizacji przedmiotu umowy jest ....., tel.....
3. Wykonawca zobowiązuje się uzgodnić z osobą wymienioną w ust 2 termin dostawy z wyprzedzeniem co najmniej 3 dniowym.
4. Zamawiający, bez jakichkolwiek roszczeń finansowych ze strony Wykonawcy z tym związanych, może odmówić przyjęcia dostawy w całości lub w części jeżeli:
   1) termin dostawy nie był z nim uprzednio uzgodniony,
   2) pracownicy Wykonawcy odmówią rozładunku przedmiotu umowy w miejscu wskazanym przez Zamawiającego.
5. Prowadzone prace wdrożeniowe i instalacyjne nie mogą zakłócać prawidłowej pracy istniejącej sieci. Wszystkie konieczne przerwy w pracy systemu muszą być zgłoszone Zamawiającemu najpóźniej na 24 godziny przed planowaną przerwą i powinny mieć miejsce poza godzinami pracy (tj. poza 8:15 -16:15 w dni robocze od poniedziałku do piątku).
6. Wykonanie przedmiotu umowy będzie potwierdzone przez upoważnionego przedstawiciela Zamawiającego w protokole dostawy/ usługi sporządzonym wg wzoru stanowiącego załącznik nr 5 do umowy.
7. Wszelkie dokumenty dotyczące dostaw/usług przygotowuje Wykonawca. Do faktury Wykonawca dołącza oryginał wypełnionego protokołu dostawy/usługi.

§6
GWARANCJA

1. Wykonawca udziela gwarancji na dostarczone urządzenia sieciowe i oprogramowanie: na okres ..... (słownie: .....) miesięcy od daty podpisania protokołu dostawy/usługi.

2. Wykonawca zapewni w okresie wskazanym w ust. 1 bezpłatny serwis naprawczy i konserwację urządzeń sieciowych w miejscu dostawy.
3. W okresie gwarancji Wykonawca może obciążyć Zamawiającego kosztami serwisu tylko wówczas, gdy uszkodzenie urządzeń nastąpiło z winy Zamawiającego.
4. Wszelkie uwagi i ewentualne reklamacje Zamawiający przekaże bezpośrednio do Wykonawcy na adres: .....
5. Powiadomienie o awarii może nastąpić tylko w dni robocze telefonicznie, faksem lub e-mailem. Po powiadomieniu zostanie dokonana nieodpłatna naprawa gwarancyjna lub wymiana urządzenia wadliwego na nowe.
6. Rozpoczęcie usuwania awarii nastąpi nie później niż następnego dnia roboczego od momentu otrzymania zgłoszenia. Zgłoszenie, które wpłynęło po godzinie 15.30 jest traktowane jako zgłoszenie przyjęte następnego dnia roboczego.
7. Usunięcie awarii nastąpi w czasie do 2 dni roboczych od momentu zgłoszenia awarii przez Zamawiającego.
8. W szczególnych przypadkach Strony mogą uzgodnić inny termin naprawy, przy czym wymagane jest potwierdzenie na piśmie.
9. W przypadku, gdy naprawa urządzeń w miejscu dostawy będzie niewykonalna lub potrwa dłużej niż 2 dni roboczych na czas naprawy zostanie dostarczone urządzenie wolne od wad (równoważne pod względem parametrów technicznych) najpóźniej 3 dnia roboczego od chwili powiadomienia o awarii.
10. Gwarancja nie ogranicza praw Zamawiającego do przenoszenia urządzeń związanego ze zmianą siedziby.

§7
WARUNKI PŁATNOŚCI

1. Płatność wynagrodzenia określonego w § 4 ust. 1 odbędzie się w ciągu 14 dni od dnia otrzymania faktur VAT, którą Wykonawca wystawi po dokonaniu protokolarnie potwierdzonego odbioru przedmiotu umowy – danego etapu, na konto Wykonawcy wskazane w fakturze.
2. Wykonawca zobowiązuje się, że do faktury dołączony będzie oryginał protokołu dostawy /usługi (sporządzony wg wzoru stanowiącego załącznik nr 5 do umowy), na którym upoważnieni przedstawiciele Zamawiającego dokonali zapisów i potwierdzeń dotyczących przedmiotu umowy za który wystawiono fakturę.
3. Wykonawca przekaże Zamawiającemu fakturę w jego centrali w Warszawie. Faktura do której nie będzie dołączony odpowiedni i kompletnie wypełniony protokół dostawy nie zostanie przez Zamawiającego zaakceptowana i będzie odesłana Wykonawcy do uzupełnienia. W takim przypadku brak zapłaty wynagrodzenia przez Zamawiającego nie będzie stanowić podstawy do naliczania odsetek ustawowych ani nie będzie traktowany jako pozostawanie w zwłoce.
4. Płatność wynagrodzenia nastąpi przelewem w ciągu 14 dni od daty otrzymania przez Zamawiającego faktury zgodnej z postanowieniami ust. 2, przy czym za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.

§8
ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

1. Strony ustalają zabezpieczenie należytego wykonania umowy w wysokości 10 % przedmiotu umowy brutto co stanowi kwotę ..... PLN (słownie: ..... PLN).
2. Zabezpieczenie zostało wniesione przez Wykonawcę przed zawarciem umowy w formie .....
3. Zabezpieczenie służy zaspokojeniu wszelkich roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania umowy przez Wykonawcę. W szczególności z zabezpieczenia Zamawiający ma prawo pokryć kary umowne.
4. Zabezpieczenie, o którym mowa w ust. 1, podlega zwolnieniu przez Zamawiającego w wysokości 70% sumy zabezpieczenia w terminie 30 dni od dnia dokonania ostatniego odbioru a 30 % tej sumy w terminie 14 dni od dnia kończącego okres gwarancyjny.

§9
KARY UMOWNE

1. Strony ustalają odpowiedzialność za niewykonanie lub nienależyte wykonanie umowy w formie kar umownych w następujących wypadkach i wysokości:
    1) Wykonawca zobowiązany jest do zapłaty kary umownej w wysokości 0,2 % wynagrodzenia umownego netto za każdy dzień zwłoki w wykonaniu przedmiotu umowy.
    2) Wykonawca zobowiązany jest do zapłaty kary umownej w wysokości 10 % wynagrodzenia umownego netto z tytułu odstąpienia od umowy z przyczyn za które ponosi odpowiedzialność Wykonawca,
    3) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 100 zł za każdy dzień opóźnienia w przypadkach o których mowa w § 6 ust 8 i 9.
2. Przez wynagrodzenie netto, będące podstawą naliczania kar umownych rozumie się wynagrodzenie w kwocie ..... PLN.
3. Zamawiający ma prawo potrącenia wartości naliczonych Wykonawcy kar umownych z należnego Wykonawcy wynagrodzenia.
4. W sytuacji, gdy kara umowna, przewidziana w ust. 1, nie pokrywa rozmiarów szkody, Zamawiającemu przysługuje prawo żądania odszkodowania na zasadach ogólnych.

§ 10
WARUNKI ODSTĄPIENIA OD UMOWY

1. Zamawiającemu przysługuje prawo do odstąpienia od umowy w terminie 30 dni od powzięcia wiadomości o następujących okolicznościach:
    1) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy,
    2) likwidacji, ogłoszenia upadłości lub rozwiązania przedsiębiorstwa Wykonawcy,
    3) nakazanego przez organ publiczny zajęcia majątku Wykonawcy,
    4) 3 – dniowej zwłoki Wykonawcy w rozpoczęciu realizacji przedmiotu zamówienia bez uzasadnionych przyczyn lub niekontynuowania jej pomimo pisemnego wezwania Zamawiającego,
    5) powierzenia przez Wykonawcę wykonania przedmiotu zamówienia osobie trzeciej bez zgody Zamawiającego,
    6) wykonywania przez Wykonawcę przedmiotu umowy wadliwie i mimo upływu wyznaczonego przez Zamawiającego terminu nie dokonania zmiany przez Wykonawcę sposobu wykonania przedmiotu umowy.
2. Odstąpienie od umowy powinno nastąpić pod rygorem nieważności na piśmie i zawierać uzasadnienie.
3. W razie odstąpienia od umowy, w terminie 7 dni od daty odstąpienia od umowy, o ile jest to możliwe w danych okolicznościach, przy udziale drugiej Strony sporządzony będzie protokół inwentaryzacji wykonania przedmiotu umowy w toku, zgodnie ze stanem faktycznym na dzień odstąpienia.

§11
POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych niniejszą umową będą miały zastosowanie przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych.
2. Ewentualne zmiany i uzupełnienia w treści umowy wymagają formy pisemnej na drodze aneksu do umowy pod rygorem nieważności.
3. Spory powstałe pomiędzy stronami wynikłe w związku z realizacją niniejszej umowy rozstrzygane będą przez sąd powszechny właściwy dla siedziby Zamawiającego.
4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Załączniki:

1. załącznik nr 1 – oferta
2. załącznik nr 2 - „Wykaz lokalizacji i miejsc dostawy urządzeń"
3. załącznik nr 3 - „Wykaz miejsc instalacji, konfiguracji i integracji urządzeń"
4. załącznik nr 4 - „Instalacja, konfiguracja oraz integracja z istniejącą infrastrukturą teleinformatyczną".

5. załącznik nr 5 – wzór protokołu dostawy/usługi.

ZAMAWIAJĄCY: **WYKONAWCA:**

Załącznik nr 5 do umowy

....., dnia ..... 2007 r.

PROTOKÓŁ DOSTAWY/USŁUGI

W dniu dzisiejszym dostarczono do Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu niżej wymieniony przedmiot umowy:

Pozycja	Nazwa przedmiotu umowy	Ilość

Zamawiający odebrał wszelką niezbędną dla w/w przedmiotu umowy dokumentację.

Zamawiający dokonał odbioru przedmiotu umowy wymienionego w protokole.

ZAMAWIAJĄCY: WYKONAWCA: