ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA CZĘŚĆ I

1. Nazwa zamówienia

Dostawa systemu DNS wraz z usługą wsparcia technicznego świadczoną przez okres 36 miesięcy.

2. Kody CPV

35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.
72250000-2 Usługi w zakresie konserwacji i wsparcia systemów.
48000000-8 Pakiety oprogramowania i systemy informatyczne.

3. Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa systemu DNS, w skład którego wchodzi: oprogramowanie wraz z licencjami, szczegółowo opisany w pkt. 5 OPZ wraz z usługami godzin eksperckich – w ramach prawa opcji, opisanymi w pkt. 7 OPZ, oraz usługą wsparcia technicznego (maintenance) opisaną w pkt. 8 OPZ.

Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Awaria	Nieprawidłowe działanie oprogramowania w szczególności brak możliwości jego używania w sposób zgodny z jego przeznaczeniem lub dokumentacją dot. systemu DNS
Godziny Robocze	Oznacza godziny od 09:00 do 17:00 w dni od poniedziałku do piątku, nie będące dniami ustawowo wolnymi od pracy na terenie Rzeczypospolitej Polskiej.
Dzień roboczy	Oznacza dzień od poniedziałku do piątku w godzinach 09:00 do 17:00 nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Roboczogodziny	Oznacza jednostkę miary czasu świadczenia Godzin eksperckich, obejmująca pracę jednej osoby przez godzinę zegarową, do której nie wlicza się czasu dojazdu do lokalizacji, w której usługa jest wykonywana.
Wirtualny Appliance	ang. Virtual Appliance oznacza oprogramowanie, które można zaimplementować na maszynie wirtualnej oraz do którego Producent dostarcza funkcjonalności systemu DNS, niezbędne licencje oraz wsparcie techniczne (maintenance).
Godziny eksperckie	Usługi konsultacji, których przedmiotem będą miedzy innymi zagadnienia wskazane w OPZ, dotyczące obsługi, konfiguracji i eksploatacji systemu DNS, bieżących problemów dotyczących jego funkcjonowania, konfiguracji, wyjaśniania wątpliwości lub

	rozwiązania zagadnień z tego zakresu przedstawianych przez Zamawiającego, związanych z obsługą systemu DNS, świadczone zdalnie, na warunkach wskazanych w OPZ (w pkt. 7), w terminach uzgodnionych zgodnie z postanowieniami Umowy również poza Dniami Roboczymi oraz poza Godzinami Roboczymi.

4. Terminy realizacji:

Termin dostawy systemu DNS wynosi - do 2 tygodni od dnia zawarcia Umowy.

5. Specyfikacja wymagań

5.1 Dostawa oprogramowania i licencji.

Przedmiotem zamówienia jest dostawa systemu DNS, w tym oprogramowania wraz z niezbędnymi licencjami, składającego się z poniższych komponentów:

- dwa Wirtualne Appliance realizujące funkcję serwera DNS Autorytatywnego - dalej DNS typ 1,
- dwa Wirtualne Appliance realizujące funkcję serwera DNS Resolver (caching) - dalej DNS typ 2,
- wirtualnej konsoli zarządzającej w/w Wirtualnymi Appliance, która musi także posiadać dodatkową instancję w postaci wirtualnej w celu zachowania redundancji.

Razem w/w komponenty składają się na system DNS, spełniający poniższe wymagania (parametry wymagane i oceniane):

Wymagania dla systemu DNS		
Lp.	**Opis wymagania**	**Parametry minimalne**
1.	Ogólne	1.1. Komponenty systemu DNS i jej mechanizmy bezpieczeństwa muszą być dostarczane przez tego samego producenta. 1.2. System DNS nie może znajdować się na liście (typu „end-of-life" oraz „end-of-support"), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025. 1.3. System DNS musi dostarczać mechanizm szyfrowania danych, który musi posiadać wsparcie dla standardów bezpieczeństwa w tym FIPS 140-2 lub FIPS 140-3 lub jego odpowiednik*.
2.	Wirtualny Appliance	2.1. System DNS musi być dostarczony w postaci Wirtualnego Appliance oraz licencji niezbędnych do uruchomienia i korzystania z wszystkich funkcjonalności systemu DNS opisanych w niniejszym OPZ, przystosowanego do uruchomienia na platformach wirtualizacji: VMWare w wersji 6 oraz 7. 2.2. System DNS musi realizować ochronę i analizowanie zapytań DNS w ramach środowiska on-premis Zamawiającego.

		**Wyjątkiem może być wymaganie opisane w ppkt. 15.3 – w tym przypadku Zamawiający będzie miał wybór skorzystania z możliwości wysyłania zapytań DNS do chmury Producenta systemu DNS (przez okres 36 miesięcy).

*Zamawiający wskazuje następujące warunki równoważności dla normy FIPS 140-2 lub 140-3 i uzna za normę równoważną opisywanej, normę która:

1) Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
2) Została wydane przez NIST (ang. National Institute of Standards and Technology) lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji,
3) Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
4) Została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa.

Wymagania szczegółowe systemu DNS		
Lp.	**Opis wymagania (funkcjonalności)**	**Parametry minimalne**
3.	Główne funkcje Systemu DNS	3.1. Musi dostarczać usługi rozwiązywania nazw domenowych przy użyciu protokołu DNS (Domain Name System). 3.2. System DNS w ramach usługi DNS musi umożliwić zarządzanie adresami IPv4 i IPv6. 3.3. Musi mieć możliwość świadczenia usługi DNS dla usług Active Directory i LDAP.
4.	Ilość zapytań DNS	Liczba zapytań obsługiwanych przez usługę DNS co najmniej 20 mln zapytań na miesiąc.
5.	Ilość stref DNS	System DNS musi umożliwiać obsługę min. 5 stref DNS.
6.	Typy rekordów DNS	System DNS musi świadczyć usługi DNS co najmniej w oparciu o rekordy DNS typu: A, NS, AAAA, CNAME, MX.
7.	Wysoka dostępność / nadmiarowość	DNS (typ 1 i 2) musi umożliwiać pracę w trybie Active/Active z drugim tożsamym komponentem DNS w celu zachowania redundancji lub wysokiej dostępności usług DNS (rozłożonych na min. dwa centra przetwarzania danych).
8.	DNSSEC	8.1. System DNS musi umożliwiać wykorzystywanie mechanizmu DNSEC w celu zapewnienie uwierzytelniania źródła danych (serwera DNS) za pomocą podpisów cyfrowych. 8.2. Musi umożliwić wsparcie usługi DNSSEC w zakresie automatycznego aktualizowania podpisów cyfrowych po zmianach dokonywanych w strefach DNS.
9.	API REST	9.1. System DNS musi zapewniać interfejs API (REST) będący integralną częścią systemu za pomocą którego możliwa jest monitorowanie i konfiguracja parametrów usługi DNS.

		9.2. Musi dostarczać mechanizm REST API do kontroli systemu, wykonywania i automatyzacji zadań wykonywanych za pomocą GUI. 9.3. Musi być dostarczona pełna dokumentacja systemu API
10.	DHCP	10.1. Musi zapewniać usługę serwera DHCP i obsługę protokołu DHCP dla IPv4 i IPv6. 10.2. Musi wspierać aktualizację danych DDNS przez usługę DHCP. 10.3. Musi wspierać funkcjonalność DHCP Failover z renegocjacją dostępnych przestrzeni adresowych. 10.4. System DNS w ramach DHCP musi zarządzać na bieżąco informacjami o przyznawaniu adresów IP i systemach, na których dany adres został przypisany (adres MAC, czas i data przyznania adresu IP).
11.	Rozszerzone kodowanie DNS	Musi posiadać wsparcie dla rozszerzonego kodowania ASCII dla rekordów DNS.
12.	Ilość obiektów w systemie DNS	System musi być przystosowany do obsługi co najmniej 400 tys. obiektów związanych z usługą DNS i DHCP.
13.	NTP (ang. Network Time Protocol)	Musi dostarczać usługę synchronizacji czasu za pomocą protokołu NTP.
14.	Ilość systemów/użytkowników podlegających ochronie za pomocą Systemu DNS	Musi umożliwić ochronę DNS dla co najmniej 500 systemów i użytkowników.
15.	DNS firewall i licencje na bazy (feed) reputacyjne	15.1. System DNS musi umożliwiać mechanizm blokowania zapytań DNS o domeny oraz adresy IP (gdy chroniony system będzie odpytywał się o domenę, która będzie rozwiązywać się na jeden z w/w adresów IP) wymienione w ppkt. od 15.2.1 - do 15.2.12 oraz system DNS musi umozliwiać poinformowanie systemu klasy SIEM (o takim zapytaniu DNS). 15.2. Producent systemu DNS zapewni przez 36 miesięcy dostęp do repozytoriów (feed), które zawierają domeny lub adresy IP kojarzone z: Wymagane: 15.2.1. adresami IP węzłów (exit node) sieci TOR. 15.2.2. domenami tworzonymi za pomocą algorytmów do generowania domen (ang. DGA). Opcjonalne[1]: 15.2.3. domenami zarejestrowanymi w ciągu ostatnich 3 dni. 15.2.4. domenami powiązanymi z atakami typu APT. 15.2.5. domenami i adresami IP powiązanymi z malware.

[1] Stanowi dodatkowe kryterium oceny Ofert

		15.2.6. domenami powiązanymi z atakami typu ransomware i innymi tego typu, które szyfrują lub są wykorzystywane jako CryptoLocker. 15.2.7. adresami IP lub domenami powiązanymi z sieciami typu Botnet lub C&C. 15.2.8. domenami powiązanymi z atakami typu phishing. 15.2.9. domenami powiązanymi z generowaniem kryptowalut. 15.2.10. domenami naśladującymi domeny (atak typu LookAlike) w celu upodobnienia nazw domenowych za pomocą użycia tzw. homografów. 15.2.11. domenami i adresami IP oferujących usługi DNS-over-HTTPS. 15.3. **System DNS powinien umożliwiać Behawioralną analizę zapytań DNS, nie tylko bazującą na feed ale na stworzonych przez Producenta algorytmach lub mechanizmach umożliwiających zaawanasowaną analizę zapytań DNS („on-premise" oraz za pomocą chmury Producenta Systemu DNS): 15.3.1. w celu ochrony przed exfiltracją danych (w zapytaniach DNS). 15.3.2. w celu weryfikacji zapytań DNS do domen typu DGA[2].
16.	Mechanizmy ochronne w DNS typ 1	16.1. Musi automatycznie chronić się (DNS typ 1) m.in. przed atakami typu: 16.1.1. Cashe-poisoning 16.1.2. Flood 16.1.3. DNS Hijacking 16.1.4. Nieautoryzowane przekierowanie domen na inne serwery DNS 16.1.5. NXDOMAIN
17.	Mechanizmy blokujące niedozwolone zapytania DNS, skategoryzowane ręcznie jako złośliwe lub niedozwolone	17.1. System DNS musi umożliwiać zastosowanie mechanizmu blokującego zapytania do niedozwolonych Hazardowych domen, które pochodzą z zewn. źródeł (innych niż producenta). 17.2. System DNS musi umożliwiać automatyczne ściąganie list (z zewn. zasobów i nie pochodzących od Producenta) z domenami i adresami IP w celu ich wykorzystania (np. blokowanie) w systemie DNS. 17.3. System DNS powinien wykrywać infiltracji z użyciem DNS i blokowania próby transferu danych zakodowanych w rekordach TXT[3].
18.	Sinkhole	Musi umożliwiać zastosowanie mechanizmu Sinkhole i przekierowania ruchu (skategoryzowanych domen jako złośliwe

[2] Stanowi dodatkowe kryterium oceny Ofert
[3] Stanowi dodatkowe kryterium oceny Ofert.

		i niedozwolone) na dowolną stronę www w celu poinformowania użytkownika korzystającego z usług DNS o zarejestrowanym zdarzeniu bezpieczeństwa.
19.	Logowanie do SIEM	19.1. Musi umożliwiać wysyłanie logów (do systemu klasy SIEM) z informacjami o: 19.1.1. audytowych (dostęp do systemy DNS), w tym próby logowania, udane i nieudane logowania. 19.1.2. zarejestrowanych niepożądanych zapytaniach DNS (dns queries). 19.1.3. zdarzenia bezpieczeństwa zarejestrowane przez system DNS. 19.1.4. o zmianach konfiguracji (dokonanych przez administratorów w systemie DNS). 19.2. Musi być możliwe dostarczenie do SIEM informacji z oryginalnym (źródłowym) adresie IP (np. z pola XFF) – co najmniej w przypadku powyższych w/w informacji z pkt. 19.1.
20.	SNMP	Komponenty systemu DNS muszą mieć możliwość monitorowania parametrów ich zasobów.
21.	Mechanizmy ułatwiające pracę grupy SOC (opcjonalne)	21.1. Dodatkowo Producent systemu DNS powinien umożliwić (co najmniej dla 5 osób) Zamawiającemu analizowanie reputacji i historii poszczególnych domen[4] za pomocą swojej (niezależnej od systemu DNS) strony www. 21.2. Producent lub system DNS powinien umożliwić eksport danych ze swoich baz reputacyjnych do wykorzystania w narzędziach klasy SIEM[5].
22.	Bezpieczna aktualizacja rekordów DDNS	Musi wspierać bezpieczną aktualizację rekordów DDNS np. za pomocą mechanizmów GSS-TSIG.
23.	Integracja (opcjonalna)	23.1. System DNS powinien umożliwiać integrację z systemami Vmware, OpenStack oraz Docker w celu automatycznego tworzenia rekordów DNS i przydzielania adresów IP[6] 23.2. System DNS powinien automatycznie tworzyć odpowiednie rekordy dla znalezionych nowych (z pkt. widzenia systemu DNS) maszyn wirtualnych[7] 23.3. W przypadku skasowania maszyny wirtualnej system powinien mieć możliwość automatycznego usuwania powiązanego z nim rekordu DNS w środowisku[8]. 23.4. Producent rozwiązania powinien udostępniać bezpłatnie narzędzie do importu danych z innych systemów DNS[9]

[4] Stanowi dodatkowe kryterium oceny Ofert.
[5] Stanowi dodatkowe kryterium oceny Ofert.
[6] Stanowi dodatkowe kryterium oceny Ofert.
[7] Stanowi dodatkowe kryterium oceny Ofert.
[8] Stanowi dodatkowe kryterium oceny Ofert.
[9] Stanowi dodatkowe kryterium oceny Ofert.

24.	Interfejsy sieciowe	Musi posiadać możliwość stworzenia i używania co najmniej czterech wirtualnych interfejsów sieciowych.
25.	Zarządzanie i konfiguracja	25.1. Zarządzanie systemem DNS musi odbywać się za pomocą Konsoli z wykorzystaniem GUI (dostępnej przez WWW) oraz za pomocą min. linii poleceń (CLI) co najmniej w przypadku systemów DNS typu 1 i 2. 25.2. Konsola musi pozwalać na równoległą pracę min. 20 administratorów (użytkowników konsoli systemu DNS) o różnych uprawnieniach. 25.3. Konsola musi umożliwiać nadawanie administratorom praw opartych o grupy i role, co pozwala na ograniczenie ich dostępu do wymaganych zasobów. Granulacja uprawnień musi umożliwiać konfigurowanie uprawnień dla pojedynczych obiektów typu sieć lub strefa DNS lub rekord DNS. 25.4. Konsola musi pełnienić funkcję zarządzania dla min. 15 komponentów systemu DNS (tego samego producenta). 25.5. Musi być zapewnione uwierzytelnianie administratorów do konsoli za pomocą: 25.5.1. bazy lokalnej 25.5.2. LDAP lub AD 25.5.3. wspracie dla protokołu RADIUS lub TACACS+ 25.6. Interfejs administracyjny DNS musi być w języku polskim lub angielskim. 25.7. Musi zapewniać możliwość zapisywania i odtworzenia (zapisanej wcześniej) konfiguracji z kopi zapasowej. 25.8. Konsola musi umożliwiać zarządzanie i konfigurację wszystkich komponentów Systemu DNS. 25.9. Komponent zarządzajacy musi umożliwiać zarządzanie DNS w tym co najmniej: 25.9.1. budowanie i dystrybucję polityk bezpieczeństwa DNS. 25.9.2. umożliwiać dystrybucję i zdalną instalację nowych wersji systemu. 25.9.3. umożliwiać sprawdzanie poprawności (monitoring typu health check) działania usługi DNS. 25.10. System DNS musi posiadać mechanizmy typu znajdowania nieużywanych adresów IPv4 i IPv6 w sieci korzystającej z Systemu DNS. 25.11. System DNS powinien umożliwiać dodawanie dodatkowych opisów dla obiektów utworzonych w systemie DNS (m.in. w rekordach dot. domen i adresów IP)[10].

[10] Stanowi dodatkowe kryterium oceny Ofert.

		25.12. System powinien posiadać mechanizm Workflow do zarządzania procesem potwierdzania i akceptacji zmian dot. rekordów DNS[11].
26.	Analityka i raportowanie	26.1. System musi umożliwić analizowanie zarejestrowanych zapytań DNS (co najmniej 500MB danych źródłowych dziennie). 26.2. Wymagana jest możliwość analizowania i rapotowania (moduł raportujący) zagadnień związanych: 26.2.1. ze zdarzeniami opisanymi w pkt. 15 (DNS firewall i licencje na bazy (feed) reputacyjne). 26.2.2. ze zdarzeniami opisanymi w pkt. 17 (Mechanizmy blokujący niedozwolone zapytania DNS, skategoryzowane ręcznie jako złośliwe lub niedozwolone). 26.2.3. z wydajnością komponentów i usługi DNS: 26.2.3.1. trend czasu odpowiedzi na zapytania DNS, 26.2.3.2. adresy IP lub domen będące źródłem największej ilości zapytań DNS, 26.2.3.3. obciążeniem zasobów np CPU, RAM, itp. 26.2.4. z czasem dostępności usługi DNS (w kontekście DNS typ 1 i 2).

6. Wymagania ogólne

1. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji ul. Królewska 27, 00-060 Warszawa.
2. Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z oprogramowania w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją chmury prywatnej na rzecz Ministra Cyfryzacji.
3. Usługa wsparcia technicznego będzie świadczona w języku polskim lub za każdorazową zgodą Zamawiającego w języku angielskim.
4. **Wykonawca zobowiązany jest dostarczyć Zamawiającemu na adres e-mail: licencje@coi.gov.pl lub do siedziby Zamawiającego w terminie do 5 Dni Roboczych od dnia zawarcia Umowy:**
   a. nośniki instalacyjne Oprogramowania, o ile nie są dostępne w formie elektronicznej;
   b. oświadczenie producenta Oprogramowania potwierdzające dostawę licencji i objęcie ich wsparciem technicznym na poziomie zgodnym z Rozdziałem 8 OPZ;
   c. adresy poczty elektronicznej, nr telefonów oraz dane dostępowe do portalu klienckiego, umożliwiające Zamawiającemu korzystanie z Wsparcia technicznego świadczonego przez producenta Oprogramowania w pełnym zakresie;

[11] Stanowi dodatkowe kryterium oceny Ofert.

d. dokumenty licencji na Oprogramowanie, w tym certyfikaty licencyjne wystawione przez producenta, umowy/standardowe warunki licencyjne producenta Oprogramowania;
e. aktualne zestawienie w formacie xlsx wszystkich dostarczonych pozycji, w zakresie Oprogramowania zawierającego informacje m.in. dotyczące numer partii, pełna nazwa produktu, metryka licencyjna, wersja i edycja oprogramowania, rodzaj licencji, okres obowiązywania licencji, okres obowiązywania wsparcia technicznego, poziom wsparcia technicznego, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto;
f. warunki Wsparcia technicznego producenta Oprogramowania.

5. **Wykonawca musi posiadać status partnera producenta Oprogramowania z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał najwyższy lub o jeden stopień niższy poziom partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta Oprogramowania. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu pierwszym chyba, że jest producentem Oprogramowania.**
6. W przypadku gdy w postępowaniu bierze udział konsorcjum jeden z Wykonawców musi posiadać status partnera.
7. Oprogramowanie na potrzeby Chmury prywatnej nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy o Krajowym systemie bezpieczeństwa (tj. Dz. U z 2018r. poz. 1560), dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, Oprogramowanie musi być zgodne z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.
8. Warunki licencji i warunki wsparcia technicznego pozostają niezmienne przez cały okres obowiązywanina Umowy w przedmiotowym postepowaniu.

7. Zasady realizowania Godzin eksperckich w ramach prawa opcji

1. Zamawiający wymaga zapewnienia przez Wykonawcę Godzin eksperckich świadczonych przez autoryzowany podmiot współpracujący bezpośrednio z producentem przedmiotu zamówienia opisanego w pkt 3 OPZ, w najwyższym lub o jeden stopień niższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta, działający w imieniu tego producenta– w wymiarze łącznie 400 Roboczogodzin, przez okres od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt 5 OPZ, do końca grudnia 2022r.
2. Osoba/y realizująca/e Godziny eksperckie musi być ekspertem w obszarze związanym z technologią dot. **systemu DNS** oraz legitymować się ważnym i aktualnym certyfikatem

Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.

3. W ramach Godzin eksperckich będzie m.in. na żądanie Zamawiającego:
   (a) opracowanie i dostarczenie projektu wdrożenia przedmiotu zamówienia, o którym mowa w pkt. 5 OPZ oraz związanej z tym wdrożeniem dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Godzin eksperckich,

   (b) opracowanie i dostarczenie procedury postępowania w razie wystąpienia incydentów bezpieczeństwa (zaejestrowanych przez system DNS).

   (c) opracowanie i dostarczenie procedury postępowania w razie błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

   (d) konsultacje i wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt. 5 OPZ,

   (e) konsultacje i wsparcie dot. utrzymania, eksploatowania, tuningu (konfiguracji i reguł/ polityk bezpieczeństwa) oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez urządzenia stanowiące przedmiot zamówienia, o którym mowa w pkt 5 OPZ,

4. Zamawiający wymaga zapewnienia realizacji Godzin eksperckich, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej z wykonawcą Umowie, ustalających przedmiot zamawianych usług, a Wykonawca będzie zobowiązany zapewnić rozpoczęcie świadczenia takich usług w terminie wskazanym w zleceniu.

8. Zasady świadczenia usług wsparcia technicznego (maitenance)

1. Wykonawca zobowiązany jest zapewnić wsparcie producenta systemu DNS lub autoryzowanego podmiotu współpracującego z producentem, przez okres 36 miesięcy, od dnia o którym mowa w pkt. 6 ppkt. 4 OPZ, z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby podmiot świadczący wsparcie posiadał najwyższy lub o jeden stopień niższy poziom partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta.
2. Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów.
3. Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych w trybie 24/7/365.
4. Zgłoszenia serwisowe będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym Awaria została zgłoszona.

9. Warunki dotyczące rozwiązań równoważnych

1. Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, lub specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym, i takim odniesieniom towarzyszą wyrazy "lub równoważne".
2. W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
3. W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.
4. W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przyapdkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.
5. Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.