ROZDZIAŁ II- OPIS PRZEDMIOTU ZAMÓWIENIA

I. Nazwa zamówienia:

Przedłużenie wsparcia technicznego producenta dla platformy NGFW Cisco FirePower oraz gwarancji wraz z zapewnieniem godzin eksperckich

II. Kody CPV:

48000000-8 Pakiety oprogramowania i systemy informatyczne
72611000-6 Usługi w zakresie wsparcia technicznego

III. Definicje

Nazwa / skrót	Opis
Dni Robocze	Dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.
Awaria	oznacza stan, w którym nie jest możliwe używanie Urządzenia w sposób zgodny z jego przeznaczeniem.
Błąd	Błąd krytyczny lub Błąd niekrytyczny
Błąd niekrytyczny	Błąd niebędący Błędem krytycznym, powodujący nieprawidłowe działanie Oprogramowania.
Błąd krytyczny	Błąd powodujący całkowity brak możliwości korzystania z Oprogramowania albo takie ograniczenie korzystania z Oprogramowania, że przestaje ono spełniać swoje podstawowe funkcje.
Godziny Eksperckie	Świadczenie, przez Wykonawcę, na podstawie zlecenia, usług dot. w szczególności integracji, konfiguracji, przygotowania skryptów, tuningu Oprogramowania, w terminach uzgodnionych z Zamawiającym, zgodnie z Umową i OPZ. Godziny Eksperckie będą świadczone przez Wykonawcę w Godzinach Roboczych. Każda Godzina Ekspercka składa się z 60 minut.
Godziny Robocze	Godziny od 9:00 do 17:00 w Dni Robocze.
Oprogramowanie	Całość lub dowolny element oprogramowania niezbędnego do prawidłowego działania Platformy. Pojęcie to obejmuje wszystkie aktualizacje i elementy przewidziane przez producenta Oprogramowania dla prawidłowego korzystania z Oprogramowania wraz z odpowiednimi Licencjami uprawniającymi do korzystania z Oprogramowania.
Lokalizacje	Dwie lokalizacje pełniące rolę ośrodków przetwarzania (Data Center) na terenie m.st. Warszawy, w których znajdują się Urządzania posiadane przez Zamawiającego.
OPZ	Niniejszy Opis Przedmiotu Zamówienia.
Platforma	Platforma NGFW Cisco FirePower 3120 składająca się z Urządzeń oraz Oprogramowania niezbędnego do ich prawidłowego działania.
Urządzenia	Dwa Urządzenia fizyczne (z ang. hardware appliance) pochodzące od producenta Cisco (model Secure Firewall 3120 Threat Defense) będące w posiadaniu Zamawiającego, wymienione w pkt IV.3. OPZ (Tabela nr 1).

Zgłoszenie	Dokonanie przez Zamawiającego zgłoszenia Awarii lub Błędu, za pomocą jednego z oficjalnych kanałów komunikacji serwisu producenta Platformy.

IV. Przedmiot zamówienia:

1. Przedłużenie wsparcia technicznego producenta (maintenance) oraz gwarancji dla posiadanej przez Zamawiającego Platformy.
2. W ramach prawa opcji zapewnienie świadczenia usługi 288 Godzin Eksperckich na zlecenie Zamawiającego, na zasadach szczegółowo opisanych w pkt VIII OPZ.
3. Wykaz Urządzeń i Licencji, których dotyczy przedłużanie wsparcia technicznego i gwarancji producenta:
   Tabela nr 1.

Lp.	Opis	Ilość	SN
1	Urządzenia: Cisco Secure Firewall 3120 Threat Defense	2	numery seryjne zostaną udostępnione na wniosek na zasadach określonych w SWZ
2	Licencje	2	Essentials, IPS

4. Zamawiający przekaże numery seryjne Urządzeń oraz opis Licencji Wykonawcom, którzy złożą do Zamawiającego wniosek o udostępnienie takich informacji, zgodnie z procedurą opisaną w rozdziale I SWZ obejmującą m.in. złożenie wniosku w formie elektronicznej wg wzoru przygotowanego przez Zamawiającego, złożenie podpisanej przez Wykonawcę umowy o zachowaniu poufności wg wzoru przygotowanego przez Zamawiającego, udostępnienie przez Zamawiającego informacji poprzez wysłanie zaszyfrowanego dokumentu za pośrednictwem poczty elektronicznej oraz hasła za pośrednictwem wiadomości SMS.

V. Termin realizacji zamówienia:

1. Wsparcie techniczne oraz gwarancja, o których mowa w pkt. IV ust. 1. OPZ, będzie świadczone przez okres 36 miesięcy od dnia odbioru wskazanego w Protokole Odbioru.
2. Dostarczenie Zamawiającemu danych i dokumentów, opisanych w pkt. VI ust. 1 OPZ, nastąpi w terminie maksymalnie 5 Dni Roboczych od daty zawarcia umowy.
3. Zamawiający ma prawo skorzystania z usługi Godzin Eksperckich w okresie, o którym mowa w pkt. 1 powyżej.

VI. Wymagania ogólne:

1. Wykonawca w terminie, o którym mowa w pkt. V ust. 2. OPZ (a także później przy każdej zmianie tych danych), prześle Zamawiającemu**:**
   a. oświadczenie producenta Platformy, potwierdzające przedłużenie wsparcia technicznego i gwarancji producenta lub zestawienie (od producenta) wszystkich komponentów Platformy, zawierającego m.in. następujące informacje: pełną nazwę i rodzaj wykupionego wsparcia technicznego, okres obowiązywania wsparcia technicznego producenta oraz gwarancji, zgodnie z zapisami zawartymi w Umowie;
   b. link lub dokument z opisem warunków wykupionego wsparcia technicznego i gwarancji;

c. Numer telefonu oraz adres email, link o którym mowa w pkt. VII.2. OPZ.

2. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży na rzecz Skarbu Państwa – Ministra Cyfryzacji. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na Skarb Państwa reprezentowany przez Ministra Cyfryzacji, z adresem korespondencyjnym przy ul. Królewskiej 27, 00-060 Warszawa, NIP 5252955037, REGON 525189465. Zamawiający lub inny podmiot wskazany przez Zamawiającego, będzie uprawniony do korzystania z przedmiotu zamówienia.
3. Przedmiot zamówienia 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 z dnia 5 lipca 2018 r. o Krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.), 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, przedmiot zamówienia musi być zgodny z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

VII. Szczegółowy opis przedmiotu zamówienia:

1. Usługi gwarancji oraz wsparcia technicznego (maintenance) dla Platformy świadczone będą przez producenta Platformy.
2. Wykonawca musi udostępnić swój numer kontaktowy i adres e-mail oraz link i dane dostępowe do portalu producenta Platformy na który będzie można zgłaszać Awarię i Błędy dotyczące Platformy. Wykonawca na prośbę Zamawiającego może być odpowiedzialny za koordynację i obsługę Zgłoszeń.
3. Wsparcie techniczne będzie świadczone w języku polskim lub angielskim, z wyjątkiem Zgłoszeń dokonanych telefonicznie, których obsługa będzie świadczona wyłącznie w języku polskim.
4. Usługa wsparcia technicznego producenta będzie realizowana na poziomie co najmniej Cisco SMARTnet Service, w tym będzie zawierać m.in:
   a. udostępnienie (wystawienie) serwisu webowego producenta Cisco (dostępnego przez Internet przez 24/7) w zakresie nowych wersji Oprogramowania, wydań uzupełniających, poprawek programistycznych, aktualnych wersji Oprogramowania, nowych wydań Oprogramowania, będących kontynuacją linii produktowej oraz portalu do obsługi zgłoszeń serwisowych,
   b. dostarczanie aktualizacji funkcjonalnych i wspierających dla Oprogramowania oraz poprawek bezpieczeństwa,
   c. dostarczanie nowych wersji Oprogramowania i technologii obejmujących m.in. poprawki serwisowe, wydania uzupełniające oraz poprawki Oprogramowania wybranych wersji produktów,
   d. dostęp za pośrednictwem serwisu www do aktualnej dokumentacji technicznej publikowanej i udostępnianej przez producenta Oprogramowania,
   e. dostęp za pośrednictwem serwisu www do obrazów (plików) do pobrania, zawierających poprawki/aktualizacje/nowe wersje Oprogramowania, niezwłocznie po ich udostępnieniu

przez producenta Oprogramowania, świadczenia całodobowej obsługi Zgłoszeń we wszystkie dni tygodnia (również w dni ustawowo wolne od pracy) elektronicznie (poprzez internetowy serwis www),

f. za datę dokonania Zgłoszenia uznaje się dzień i godzinę dokonania Zgłoszenia przez Zamawiającego,
g. przygotowanie i przedstawienie Zamawiającemu rozwiązania usunięcia Błędu krytycznego najpóźniej w ciągu 24 godzin od chwili Zgłoszenia Błędu krytycznego,
h. przygotowanie i przedstawienie Zamawiającemu rozwiązania usunięcia Błędu niekrytycznego najpóźniej w ciągu 5 Dni Roboczych od chwili Zgłoszenia Błędu niekrytycznego,
i. Wykonawca zobowiązuje się do informowania Zamawiającego (na adres: security@cyfra.gov.pl) o pojawieniu się krytycznych poprawek bezpieczeństwa w terminie 1 Dnia Roboczego od dnia ich publikacji.

5. Usługa gwarancji producenta będzie realizowana na poziomie co najmniej Smart Net Total Care 24x7x4 z opcją Disk Retention (dyski z Urządzeń zostają u Zamawiającego), w tym będzie zawierać m.in:
   a. dostarczenie części zamiennej lub podmiana wadliwego komponentu Urządzeń lub Urządzenia w terminie nie później niż 4 godziny od momentu dokonania Zgłoszenia (przez 24h, 7 dni w tygodniu w tym uwzględniając także dni świąteczne).
   b. możliwość wymiany dowolnego komponentu Urządzenia lub całego Urządzenia po decyzji otrzymanej bezpośrednio od producenta Platformy (support Cisco). W ramach gwarancji na Zamawiającego przenoszona jest własność wymienionego komponentu Urządzenia lub Urządzenia.
   c. procedurę RMA (ang. Return Merchandise Authorization) koordynuje i uruchamia producent Cisco lub Wykonawca.
   d. koszty dostarczenia wymienianego komponentu Urządzenia lub Urządzenia ponosi Wykonawca lub producent Platformy.
   e. obsługa Zgłoszeń Awarii ma być realizowana za pośrednictwem portalu producenta Platformy (m.in. za pomocą serwisu webowego dostępnego przez Internet przez 24/7).
   f. usługi w ramach Gwarancji będą świadczone zdalnie lub w przypadku konieczności we wskazanych Lokalizacjach.
6. Zamawiający wymaga, aby Wykonawca posiadał najwyższy lub o jeden stopień niższy status partnera producenta Urządzeń na terenie Polski. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa w zdaniu poprzednim.

VIII. Zasady realizacji Godzin Eksperckich:

1. W ramach realizacji zamówienia Zamawiającemu przysługuje możliwość skorzystania z 288 Godzin Eksperckich. Prace będą realizowane w Godzinach Roboczych, na podstawie zapotrzebowania zgłoszonego przez Zamawiającego, zgodnie z procedurą wskazaną w Umowie.
2. Osoba realizująca usługi w ramach Godzin Eksperckich musi być ekspertem w obszarze związanym z technologią NGFW, posługiwać się językiem polskim lub angielskim oraz na żądanie Zamawiającego legitymować się certyfikatem producenta lub akredytowanego przez producenta podmiotu, potwierdzającym ww. wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego producenta.

3. Godziny eksperckie będą świadczone zdalnie lub w przypadku konieczności we wskazanych Lokalizacjach lub siedzibie Zamawiającego.
4. W ramach Godzin Eksperckich będą świadczone na żądanie Zamawiającego w szczególności następujące usługi:
   a. opracowanie i dostarczenie projektu wdrożenia/rekonfiguracji/rozwoju w zakresie Platformy oraz związanej z tym dokumentacji powykonawczej, a także przeniesienie majątkowych praw autorskich do utworów wytworzonych w toku wykonywania Godzin Eksperckich,
   b. konsultacje i wsparcie w konfiguracji Platformy,
   c. opracowanie i dostarczenie dokumentów, procedur i instrukcji, dotyczących m.in.:
      (i) postępowania w razie wystąpienia incydentów bezpieczeństwa,
      (ii) postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,
      (iii) instalacji, konfiguracji oraz parametryzacji wdrożonej Platformy,
      (iv) wykonania kopii bezpieczeństwa i ich odtworzenia,
      (v) aktualizacji i wdrażania poprawek do Oprogramowania,
   d. wsparcie pracowników Zamawiającego w użytkowaniu Platformy oraz implementacja nowych funkcjonalności lub modyfikacja już skonfigurowanych,
   e. wsparcie w przypadku wystąpienia incydentu bezpieczeństwa:
      (i) wsparcie w zakresie wykonania analizy wykorzystanych podatności,
      (ii) kontakt z ekspertem Cisco w zakresie bezpieczeństwa Platformy,
      (iii) analiza zakresu kompromitacji systemu,
      (iv) wsparcia w konfiguracji/rekomendacji w celu zabezpieczenia Platformy,
      (v) wsparcie w zakresie usunięcia skutków oraz rozwiązania incydentu bezpieczeństwa,
   f. wsparcie w planowanych pracach serwisowych:
      (i) przeprowadzania aktualizacji komponentów Platformy,
      (ii) weryfikacja poprawności konfiguracji Platformy
      (iii) konsultacji w czasie prac serwisowych;
   g. wsparcie w obsłudze zgłoszeń serwisowych (w tym także kontakt z Cisco w imieniu Zamawiającego).
   h. przeprowadzenie warsztatów z technologii Firepower.

IX. **Pozostałe wymagania opisane zostały w Projektowanych Postanowieniach Umowy (zawartych w rozdziale III SWZ).**