Warszawa, dnia 30.06.2021 r.

Strona WWW

WYJAŚNIENIA I ZMIANY SWZ NR 6

Dotyczy: „Dostawa sprzętu i oprogramowania wraz ze wsparciem technicznym (4 części)", w zakresie części III - *Rozbudowa systemu IBM Qradar poprzez dostawę sprzętu i licencji wraz z usługami wsparcia technicznego i gwarancją* oraz części IV - *Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją*" - COI-ZAK.262.4.2021

Zamawiający, działając na podstawie art. 135 ust. 2 i art. 137 ust. 1 ustawy z 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2019 r., poz. 2019 późn. zm.) – dalej: ustawa Pzp, przedstawia poniżej treść wyjaśnień oraz zmianę SWZ:

Pytanie 1
Jakie są pozostałe wymagania na procesory - poza tym że maja mieć 12 rdzeni każdy?

ODPOWIEDŹ:

W zakresie wymagania opisanego w pkt III. 2.1 wiersz „Procesor" Rozdział II – Opis Przedmiotu Zamówienia dla części III przedmiotowego zamówienia, Zamawiający wyjaśnia, że w pkt II. opisał przedmiot zamówienia, wskazując tzw. produkt referencyjny, natomiast w pkt II.2.1. opisał kryteria stosowane w celu oceny równoważności, obejmujące parametry minimalne, których spełnienia wymaga od oferowanego produktu równoważnego.

Pytanie 2
Czy w opisie równoważności, w sekcji dyski zawarto prawidłowy opis dysków? Czy Zamawiający uzna wymaganie za spełnione jeżeli zostanie zaoferowany sprzęt wyposażony w 12 sztuk dysków 8TB 7.2K SAS 12Gb oraz kontroler RAID 930-16i 4GB?

ODPOWIEDŹ:

W zakresie wymagania opisanego w pkt III. 2.1 wiersz „Dyski" Rozdział II – Opis Przedmiotu Zamówienia dla części III przedmiotowego zamówienia, Zamawiający uzna wymaganie za spełnione, jeżeli zostanie zaoferowany sprzęt wyposażony w 12 sztuk dysków 8TB 7.2K SAS 12Gb oraz kontroler RAID 930-16i 4GB. Zgodnie z postanowieniem pkt 4.2 Rozdziału I SWZ, „Wszystkie wymagania określone w rozdziale II SWZ – Opis przedmiotu zamówienia stanowią wymagania minimalne, a ich spełnienie jest obligatoryjne – z wyjątkiem wymagań wyraźnie oznaczonych jako przedmiot kryterium oceny ofert.".

Pytanie 3
Prosimy o uszczegółowienie wymagań dotyczących kart/portów FC. Czy Zamawiający uzna za spełniający wymagania sprzęt wyposażony w jedną dwuportową kartę FC 16Gb?

ODPOWIEDŹ:

W zakresie wymagania opisanego w pkt III. 2.1 wiersz „Karty sieciowe" Rozdział II – Opis Przedmiotu Zamówienia dla części III przedmiotowego zamówienia Zamawiający uzna za spełnienie wymagania gdy sprzęt będzie wyposażony w jedną dwuportową kartę FC 16Gb.

Pytanie 4

Wykonawca wnosi o zmodyfikowanie definicji Zlecenia, w taki sposób aby była zgodna z zapisami umowy wskazanymi w par. 2 ust. 1 pkt 2 oraz par. 5 ust 3 tj. aby brzmiała:
„Dokument w formie pisemnej (w tym w formie elektronicznej, opatrzonej ważnym kwalifikowanym podpisem elektronicznym), na podstawie którego Zamawiający wskazuje zakres oraz termin prac do wykonania, a które Wykonawca zobowiązuje się zapewnić, że zostaną wykonane jako Godziny eksperckie, sporządzony zgodnie ze wzorem, stanowiącym Załącznik nr 7 do Umowy.” Zobowiązaniem Wykonawcy jest zapewnienie wykonania przedmiotu Zlecenia.

ODPOWIEDŹ:

Zamawiający informuje, że dokonał zmiany postanowienia § 1 wiersz 23 Tabeli, w Rozdziale III - Projektowane postanowienia umowy – część 3: Rozbudowa systemu IBM Qradar poprzez dostawę sprzętu i licencji wraz z usługami wsparcia technicznego i gwarancją oraz Rozdziale III - Projektowane postanowienia umowy – część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, w następującym zakresie:

Przed zmianą:

„Dokument w formie pisemnej (w tym w formie elektronicznej, opatrzonej ważnym kwalifikowanym podpisem elektronicznym), na podstawie którego Zamawiający zobowiązuje się powierzać Wykonawcy wykonywanie Godzin eksperckich, wskazujący zakres oraz terminy prac, które Wykonawca zobowiązuje się wykonywać jako Godziny eksperckie, sporządzony zgodnie ze wzorem, stanowiącym Załącznik nr 7 do Umowy.”

Po zmianie:

„Dokument w formie pisemnej (w tym w formie elektronicznej, opatrzonej ważnym kwalifikowanym podpisem elektronicznym) - na podstawie którego Zamawiający zobowiązuje się powierzać Wykonawcy wykonywanie Godzin eksperckich, wskazujący zakres oraz terminy prac, których terminową realizację, jako Godzin eksperckich, zobowiązany jest zapewnić Wykonawca - sporządzony zgodnie ze wzorem, stanowiącym Załącznik nr 7 do Umowy.”.

Pytanie 5

Wykonawca wnosi o modyfikację treści par. 2 ust1. W taki sposób, aby brzmiał:
„1. Przedmiotem Umowy jest:
1) dostawa do Lokalizacji i przeniesienie na Zamawiającego własności Sprzętu wraz z Dokumentacją oraz zapewnienie udzielenia licencji niezbędnych do prawidłowego funkcjonowania Sprzętu i zapewnieniem przez Wykonawcę Gwarancji dla Sprzętu wraz z zapewnieniem przez Wykonawcę Wsparcia producenta dla Licencji i Oprogramowania
2) zapewnienie przez Wykonawcę świadczenia Godzin eksperckich na rzecz Zamawiającego”
Przeniesienie własności licencji oraz udzielenia licencji może dokonać tylko producent oprogramowania. Wykonawca może zapewnić jedynie udzielenie licencji przez producenta.

ODPOWIEDŹ:

Zamawiający informuje, że dokonał zmiany wskazanego w pytaniu postanowienia SWZ czynnością z dnia 15.06.2021 „Wyjaśnienia i zmiany SWZ nr 1”.

Pytanie 6

Wykonawca wnosi o zmianę treści par. 4 ust. 1 pkt 7 w taki sposób, aby brzmiał:
„Według jego najlepszej wiedzy licencje oraz jakiekolwiek inne przekazane utwory, nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów, ani praw do baz danych ani nie będą ograniczać korzystania z nich oraz będą zgodne z Umową i będą realizowały wszystkie funkcjonalności opisane w Umowie;”

1. Oświadczenie i gwarancję o nienaruszaniu praw własności intelektualnej osób trzecich może przekazać właściciel licencji.

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na proponowaną zmianę postanowień SWZ. Zamawiający oczekuje, że Wykonawca, z którym zostanie zawarta umowa w sprawie zamówienia publicznego, będzie odpowiedzialny wobec Zamawiającego, za wykonanie dostawy takich licencji i jakichkolwiek innych utworów, z których korzystanie nie będzie naruszać praw osób trzecich, nie tylko na podstawie przytoczonego w pytaniu oświadczenia, ale również z tytułu rękojmi za ewentualne wady prawne dostarczanych licencji lub utworów.

Pytanie 7

Wykonawca wnosi o zmianę treści par. 5 ust 6 w taki sposób, aby brzmiał:
„Po zakończeniu prac na podstawie Zlecenia, Strony zobowiązują się potwierdzić fakt ich wykonania w formie pisemnej (lub poprzez zastosowanie ważnego, kwalifikowanego podpisu elektronicznego), zgodnie ze wzorem stanowiącym Załącznik nr 8 do Umowy”
Nie można z góry stwierdzić, że prace w ramach Zleceń będą realizowane przez Wykonawcę. Zadaniem Wykonawcy jest zapewnienie wykonania przedmiotu Zlecenia.

ODPOWIEDŹ:

Zamawiający informuje, że dokonał zmiany postanowienia § 5 ust. 6, w Rozdziale III - Projektowane postanowienia umowy – część 3: Rozbudowa systemu IBM Qradar poprzez dostawę sprzętu i licencji wraz z usługami wsparcia technicznego i gwarancją oraz Rozdziale III - Projektowane postanowienia umowy – część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, w następującym zakresie:

Przed zmianą:

„Po zakończeniu prac, zrealizowanych przez Wykonawcę na podstawie Zlecenia, Strony zobowiązują się potwierdzić fakt ich wykonania w formie pisemnej (lub poprzez zastosowanie ważnego, kwalifikowanego podpisu elektronicznego), zgodnie ze wzorem stanowiącym Załącznik nr 8 do Umowy”

Po zmianie:

„Po zakończeniu prac, zrealizowanych na podstawie Zlecenia, Strony zobowiązują się potwierdzić fakt ich wykonania w formie pisemnej (lub poprzez zastosowanie ważnego, kwalifikowanego podpisu elektronicznego), zgodnie ze wzorem stanowiącym Załącznik nr 8 do Umowy”.

Pytanie 8

Wykonawca wnosi o zmianę treści par. 7 ust. 1 pkt 3 w taki sposób, aby brzmiał:
„Według jego najlepszej wiedzy Oprogramowanie, jego aktualizacje/poprawki oraz inne utwory przekazane w ramach realizacji Umowy, nie będą naruszać praw własności intelektualnej osób trzecich, w tym praw autorskich, patentów”
1) Oświadczenie i gwarancję o nienaruszaniu praw własności intelektualnej osób trzecich może przekazać właściciele licencji.

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na proponowaną zmianę postanowień SWZ. Zamawiający oczekuje, że Wykonawca, z którym zostanie zawarta umowa w sprawie zamówienia publicznego, będzie odpowiedzialny wobec Zamawiającego, za wykonanie dostawy Oprogramowania oraz jego aktualizacji/poprawek czy innych utworów, z których korzystanie nie będzie naruszać praw osób trzecich, nie tylko na podstawie przytoczonego w pytaniu oświadczenia, ale również z tytułu rękojmi za ewentualne wady prawne dostarczanych przedmiotów zamówienia.

Pytanie 9

W związku z faktem, że umowa nie stanowi dokumentu gwarancyjnego uprawniającego do skorzystania z uprawnień gwarancyjnych, a dokumentem takim jest ……
Wykonawca wnosi o modyfikacje treści par 8 ust 3 w taki sposób, aby brzmiał:
1. „Wykonawca oświadcza, że ……. Stanowi dokumenty gwarancyjny bez konieczności składania dodatkowego dokumentu na okoliczność udzielenia Gwarancji."

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na proponowaną zmianę. W pkt iii.4.(1) Zamawiający wskazał, że wymaga, aby gwarancja dla dostarczanych urządzeń była udzielana przez ich producenta „lub autoryzowany podmiot współpracujący z Producentem" i niezależnie od treści ewentualnych dokumentów udostępnianych przez Producenta razem z Urządzeniem, Zamawiający wymaga, aby treść Gwarancji obejmowała co najmniej wymogi, wskazane w umowie ws zamówienia publicznego.

Pytanie 10

Wykonawca wnosi o modyfikacje treści par. 12 ust 9 w taki sposób, aby brzmiał:
„Obowiązek zachowania poufności nie dotyczy informacji żądanych przez uprawnione organy, w zakresie w jakim te organy są uprawnione do ich żądania, zgodnie z obowiązującymi przepisami prawa. W takim przypadku Strony zobowiązane są wzajemnie poinformować się za pośrednictwem osoby sprawującej nadzór nad realizacją Umowy wskazanej w § 16 ust. 1 Umowy o żądaniu takiego organu, przed ujawnieniem informacji"
1. Umowa przewiduje obowiązek zachowania w tajemnicy zarówno informacji poufnych Zamawiającego jak i Wykonawcy. Stąd obowiązek poinformowania o żądaniu ujawnienia informacji poufnej przez uprawnione ograny powinien ciążyć zarówno na Wykonawcy jak i na Zamawiającym.

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na proponowaną zmianę.

Pytanie 11

Wykonawca wnosi o modyfikacje treści par. 12 ust 10 w taki sposób, aby brzmiał:
„Udostępnianie, ujawnianie, przekazywanie, powielanie oraz kopiowanie przez którąkolwiek ze Stron Umowy dokumentów, zawierających informacje związane z realizacją Umowy, lub samych informacji, z wyjątkiem przypadków, w jakich jest to konieczne w celu jej realizacji, wymaga zgody Strony, której informacje dotyczą".
1. Umowa przewiduje obowiązek zachowania w tajemnicy zarówno informacji poufnych Zamawiającego jak i Wykonawcy. Stąd obowiązek uzyskania zgodny na ujawnienie informacji poufnej którejś ze Stron umowy powinien być obustronny.

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na proponowaną zmianę.

Pytanie 12

Wykonawca wnosi o usunięcie treści par. 13 ust. 5 pkt 7 w związku z faktem, iż par. 5 ust. 4 zd. 2 nie wskazuje żadnego terminu. Tym samym naliczenie kary umownej wskazanej w par. 13 ust. 5 pkt 7 jest bezprzedmiotowe.

ODPOWIEDŹ:

Zamawiający informuje, że dokonał zmiany wskazanego w pytaniu postanowienia SWZ czynnością z dnia 15.06.2021 „Wyjaśnienia i zmiany SWZ nr 1".

Pytanie 13
Wnosimy o wykreślenie w pkt. 2.2.13. tekstu w wierszach 5-7: „o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania danych, skierowanej do Dalszego Procesora"

ODPOWIEDŹ:
Zamawiający nie wyraża zgody na proponowaną zmianę Załącznika „Wzór – Umowa powierzenia przetwarzania danych osobowych" do Rozdziału nr III SWZ w zakresie żadnej z części. Zamawiający jako podmiot przetwarzający zgodnie z treścią art. 28 ust. 4 RODO jak również treścią zawartej z Administratorem danych osobowych umowy powierzenia przetwarzania danych nie może dowolnie zmieniać treści umowy dalszego powierzenia przetwarzania danych.

Pytanie 14
Zwracamy się do Zamawiającego o zmianę w pkt. 8 Umowy PDO, ppkt. 8.2 poprzez zmianę zapisu na „bez zbędnej zwłoki, jednak nie później niż w ciągu 72 godzin od wykrycia naruszenia.." Zamiast 8 godzin.

ODPOWIEDŹ:
Zamawiający nie wyraża zgody na proponowaną zmianę Załącznika „Wzór – Umowa powierzenia przetwarzania danych osobowych" do Rozdziału nr III SWZ w zakresie żadnej z części. Zamawiający jako podmiot przetwarzający zgodnie z treścią art. 28 ust. 4 RODO jak również treścią zawartej z Administratorem danych osobowych umowy powierzenia przetwarzania danych nie może dowolnie zmieniać treści umowy dalszego powierzenia przetwarzania danych.

Pytanie 15
Zwracamy się do Zamawiającego o pozostawienie w pkt. 9.9 pierwszego zdania tj. „9.9. Dalszy Procesor ponosi względem Procesora odpowiedzialność na zasadach ogólnych do wysokości rzeczywistej szkody, z wyłączeniem utraconych korzyści." I wnosimy o wykreślenie pozostałej części ppkt. 9.9.

ODPOWIEDŹ:
Zamawiający nie wyraża zgody na proponowaną zmianę Załącznika „Wzór – Umowa powierzenia przetwarzania danych osobowych" do Rozdziału nr III SWZ w zakresie żadnej z części. Zamawiający jako podmiot przetwarzający zgodnie z treścią art. 28 ust. 4 RODO jak również treścią zawartej z Administratorem danych osobowych umowy powierzenia przetwarzania danych nie może dowolnie zmieniać treści umowy dalszego powierzenia przetwarzania danych.

Pytanie 16
Wnosimy o wykreślenie całego ppkt. 9.10

ODPOWIEDŹ:
Zamawiający nie wyraża zgody na proponowaną zmianę Załącznika „Wzór – Umowa powierzenia przetwarzania danych osobowych" do Rozdziału nr III SWZ w zakresie żadnej z części. Zamawiający jako podmiot przetwarzający zgodnie z treścią art. 28 ust. 4 RODO jak również treścią zawartej z Administratorem danych osobowych umowy powierzenia przetwarzania danych nie może dowolnie zmieniać treści umowy dalszego powierzenia przetwarzania danych.

Pytanie 17
Zwracamy się z prośbą do zamawiającego o odpowiedzi na następujące pytania:
Ad. Umowa główna
Pytanie do Zamawiającego odnośnie zapisów paragrafu 8 Umowy tj. „ 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. Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z oprogramowania, dostarczonego na podstawie umowy, w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją chmury prywatnej na rzecz Ministra Cyfryzacji."
Co oznacza powyższy zapis na etapie obecnego postępowania?
Czy end userem będzie COI?
Czy end userem z prawem do licencji będzie Minister Cyfryzacji?

ODPOWIEDŹ:

Zamawiający wyjaśnia, że zgodnie ze statutem COI organem pełniącym funkcję organu założycielskiego COI jest minister właściwy do spraw informatyzacji. COI jako jednostka sektora finansów publicznych została utworzona do realizacji zadań publicznych pozostających we właściwości Skarbu Państwa – Ministra Cyfryzacji, „MC". COI na zlecenie MC prowadzi działania zakupowe zamawiając usługi i dostawy w celu realizacji zobowiązań wynikających z umów zawartych z MC. Biorąc pod uwagę, że COI zapewnia MC usługi zewnętrzne do OPZ został wprowadzony zapis zgodnie z którym wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim jest MC. Zamawiający wymaga więc uruchomienia rejestracji licencji na użytkownika końcowego jakim jest MC. Zatem, MC nie będzie dokonywało dalszej odsprzedaży, ponieważ zgodnie z brzmieniem wymogu ww. dokumenty mają być wystawione od razu na rzecz MC. Z powyższego wymogu nie wynika również obowiązek sublicencjonowania. Zamawiający wymaga, aby COI i MC uzyskali na podstawie licencji prawo do korzystania na zasadach określonych szczegółowo w SWZ, a w szczególności w umowie. Zamawiający wyjaśnia, że przez „dalszą odsprzedaż" rozumie wyłącznie wewnętrzny proces księgowy, który w żaden sposób nie wpływa na warunki licencjonowania producentów, ani nie zmienia przeznaczenia niniejszego zamówienia.

Zamawiający pragnie zauważyć, że zgodnie z jego najlepszą wiedzą powyższe nie wymaga zaoferowania specjalnie negocjowanych warunków licencyjnych na potrzeby realizacji przedmiotowego zamówienia. Zamawiający przeprowadził do tej pory liczne zamówienia, których przedmiotem była dostawa licencji oraz sprzętu wiodących producentów (np. IBM, Oracle, Redhat, Vmware, Microsoft) stosując ww. wymóg i nigdy nie spotkał się z zarzutem braku możliwości jego zrealizowania.

Zamawiający wskazuje również, że zgodnie z Rozporządzeniem Rady Ministrów z dnia 7 października 2020 r. Poz. 1730 w sprawie zniesienia Ministerstwa Cyfryzacji, zniesiono Ministerstwo Cyfryzacji, a pracownicy dotychczasowego Ministerstwa Cyfryzacji obsługujący sprawy działu informatyzacja zostali włączeni do Kancelarii Prezesa Rady Ministrów. Zakres działania Ministra Cyfryzacji został natomiast określony w Rozporządzeniu Prezesa Rady Ministrów z dnia 6 października 2020 r. Poz. 1716 w sprawie szczegółowego zakresu działania Ministra Cyfryzacji, zgodnie z którym Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, a jego obsługę zapewnia Kancelaria Prezesa Rady Ministrów. Zamawiający słusznie zatem wskazał w ww. wymogu, że docelowym licencjobiorcą ma być Minister Cyfryzacji jako *statio fisci* Skarbu Państwa. Ponadto, jak wyżej wskazano Zamawiający prowadzi działania zakupowe w celu realizacji zobowiązań wynikających z umów zawartych ze Skarbem Państwa – Ministrem Cyfryzacji.

Jednakże, w celu sprecyzowania wymagań, Zamawiający dokonuje zmiany powyższego wymogu, który otrzymuje brzmienie:

„Niniejszy zakup jest dokonywany na rzecz klienta końcowego jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji. Wobec tego przedmiot zamówienia jest przeznaczony do jednorazowej dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp.

muszą być wystawione na docelowego licencjobiorcę (klienta końcowego) jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji, ul. Królewska 27, 00-060 Warszawa".

Pytanie 18

W dokumencie Rozdział 1 SWZ w punkcie 5 Termin wykonania zamówienia, Zamawiający specyfikuje m.in. maksymalne czasy dostaw dla zamawianych rozwiązań. Dla części 3 Zamawiający specyfikuje 8 tygodni. Dla części 4, Zamawiający specyfikuje 4 tygodnie.
W obecnej sytuacji z brakami na rynku komponentów elektronicznych oraz metali rzadkich wnosimy o wyrównanie terminów dostaw dających równe szansę na przygotowanie oferty dla producentów, którzy produkują swoje urządzenia na tzw. stock, oraz dla producentów, którzy produkują pod konkretne zamówienie klienta. Prosimy o zmianę terminu dostaw dla części 4 NGFW na 7 tygodni (we wszystkich dokumentach – SWZ, wzór umowy itp.).

ODPOWIEDŹ:

Zamawiający wyraża zgodę na przedmiotową zmianę. Zamawiający informuje, że dokonał zmiany SWZ w zakresie opisanego w pytaniu terminu dostawy NGFW.

Pytanie 19

W punkcie „19.10 Zasady oceny kryterium „Dodatkowa funkcjonalność" (DF) w zakresie części 4" Zamawiający opisuje dodatkowo punktowane funkcjonalności. W trzech pierwszych punktach, następuje mało precyzyjna definicja profili Common Criteria w połączeniu z frazą „lub równoważne":
Zgodność NGFW z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub równoważnym. (5 pkt.)
Zgodność NGFW i Konsoli Zarządzającej z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile for Network Devices v2.1" lub równoważnym. (24 pkt.)
Zgodność NGFW z profilem zabezpieczeń Common Criteria – „PP-Module for Virtual Private Network (VPN) Gateways" lub równoważnym. (5 pkt).
Ponieważ zapisy te, stanowią znaczną większość opcjonalnej oceny punktowej prosimy o precyzyjne określenie wymagań w zakresie wersji danych profili. W obecnej formie urządzenia posiadające certyfikację CC dla starszych wersji profili (np. 1.0 zamiast 2.1 dla Network Devices) otrzymają taką samą ilość punktów co urządzenia posiadające profil ND w wersji 2.1. Prosimy o uszczegółowienie, czy podana wersja jest to minimalna wersja profili Common Criteria akceptowana przez Zamawiającego?

ODPOWIEDŹ:

Zamawiający wyraża zgodę na przedmiotową zmianę. Zamawiający informuje, że dokonał zmiany SWZ w zakresie opisanego w pytaniu sposobu oceny ów, opisanych w pkt 19.10.1-19.10.7 Rozdziału I SWZ.

Pytanie 20

W wymaganiu 3.5 dla NGFW (str. 5 pdf) Zamawiający definiuje wymaganie:
„3.5 NGFW lub Konsola Zarządzająca musi dostarczać mechanizm szyfrowania danych, który będzie posiadał odpowiednie certyfikacje FIPS 140-2 lub 140-3 lub równoważny*."
Prosimy o wyjaśnienie:
- Czy wszystkie elementy oferowane w ramach części 4 (tj. wszystkie NGFW oraz Konsola Zarządzania) mają posiadać certyfikację FIPS, czy może tylko jedno z elementów systemu – albo urządzenia NGFW, albo Konsola Zarządzania?
- Część producentów wymaga specjalnej licencji albo opłaty za możliwość uruchomienia urządzeń w trybie FIPS. Czy zamawiający planuje uruchomić urządzenia w trybie FIPS i należy dostarczyć opcjonalne wyposażenie np. licencje, obudowy, osłony, blokady itp.?

ODPOWIEDŹ:

Zamawiający podtrzymuje wymaganie z pkt 3.5 Opisu przedmiotu zamówienia. Mechanizm szyfrowania danych (certyfikacje FIPS 140-2 lub 140-3 lub równoważny) musi być możliwy do wykorzystania przez Zamawiającego.

Pytanie 21

W wymaganiu dla NGFW w punkcie 14.1 Zamawiający definiuje: „Musi zapewniać filtrowanie w oparciu o kategorie jak Adult, Gambling, Social Networking, video stream oraz Malware, Phishing, C&C, TOR, Proxy anonimizujące, itp.,"
Czy jest to lista przykładowa kategorii czy wymagana?

ODPOWIEDŹ:

Zamawiający podtrzymuje wymaganie z pkt 14.1 Opisu przedmiotu zamówienia. Przywołane w pytaniu postanowienie OPZ wskazuje, że wymienione w nim funkcjonalności „muszą być zapewnione" przez oferowane urządzenie.

Pytanie 22

W wymaganiu dla NGFW w punkcie 14.1 Zamawiający definiuje: „Musi zapewniać filtrowanie w oparciu o kategorie jak Adult, Gambling, Social Networking, video stream oraz Malware, Phishing, C&C, TOR, Proxy anonimizujące, itp.,"
Różni producenci w różny sposób realizują technologie filtrowania sieci TOR. Realizacja tej funkcji tylko za pomocą URL nie jest efektywna i nie przynosi odpowiednich rezultatów. Zwłaszcza przy braku możliwości rozszyfrowania komunikacji filtracja na poziomie URL dla TOR i Proxy nie będzie działać prawidłowo.
Czy realizacja np. filtrowania np. TOR lub np. Proxy może być realizowana za pomocą funkcji „feeds" z wymagania 15.5?

ODPOWIEDŹ:

Zamawiający podtrzymuje wymaganie z pkt 14.1 Opisu przedmiotu zamówienia. Dozwolony jest każdy mechanizm kategoryzujący ruch sieciowy pod warunkiem, że zapewni jego filtrowanie przez NGFW.

Pytanie 23

W wymaganiu dla NGFW w punkcie 16.4 Zamawiający definiuje wymaganie obsługi reakcji IPS jako „16.4 Dla wskazanych IP (podsieci) i/lub stref bezpieczeństwa musi być możliwość definiowania różnych (16.1-16.3) w/w reakcji."
Wymaganie to jest cechą charakterystyczną rozwiązań Firepower producenta firmy Cisco.
W rozwiązaniach producentów NGFW reakcje tego typu definiowane są za pomocą profili łączonych z Politykami Bezpieczeństwa. Konfiguracja taka jest bardziej elastyczna i pozwala na bardziej precyzyjne definiowanie sposobu zachowania się urządzeń Firewall.
Prosimy o zmianę wymagania oraz akceptację obu trybów konfigurowania oczekiwanej funkcjonalności.

ODPOWIEDŹ:

Zamawiający informuje, że dokonał zmiany postanowienia pkt III.1.2 ppkt 16.4 w Rozdziale II – Opis przedmiotu zamówienia –część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, w następującym zakresie:

Przed zmianą:

„16.4 Dla wskazanych IP (podsieci) i/lub stref bezpieczeństwa musi być możliwość definiowania różnych (16.1-16.3) w/w reakcji."

Po zmianie:
„16.4 Dla wskazanych IP (podsieci) lub stref bezpieczeństwa musi być możliwość definiowania różnych reakcji (16.1-16.3) lub profili IPS oraz różnych konfiguracji polityk bezpieczeństwa."

Pytanie 24
W wymaganiu 22.5 dla NGFW (str. 11 pdf) Zamawiający definiuje wymaganie: „22.5 Musi być możliwość sprawdzenia wpływu na chroniony ruch sieciowy nowych sygnatur IPS bez konieczności ich zatwierdzenia na NGFW."
Czy Zamawiający zaakceptuje rozwiązanie, w którym istnieje możliwość sprawdzenia wpływu aktualizacji rozpoznawanych przez system NGFW aplikacji (bezpośrednio na urządzeniu NGFW) będzie zaakceptowana jako spełniająca te wymaganie?
Czy Zamawiający zaakceptuje jako spełnienie tego wymagania mechanizm powiadamiania przez producenta o aktualizacjach sygnatur i aplikacji dostępny w GUI systemu jako dziennik aktualizacji (tzw. release notes) w połączeniu z dodatkowym bezpośrednim powiadamianiem za pomocą wiadomości wysyłanych przez producenta rozwiązania?

ODPOWIEDŹ:
Zamawiający informuje, że dokonał zmiany postanowienia pkt III.1.2 ppkt 22.5 w Rozdziale II – Opis przedmiotu zamówienia –część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, w następującym zakresie:
Przed zmianą:
„22.5 Musi być możliwość sprawdzenia wpływu na chroniony ruch sieciowy nowych sygnatur IPS bez konieczności ich zatwierdzenia na NGFW."
Po zmianie:
„22.5 Powinna być możliwość sprawdzenia wpływu na chroniony ruch sieciowy nowych sygnatur IPS bez konieczności ich zatwierdzenia na NGFW, tzn. przed włączeniem nowych sygnatur IPS z trybem blokowania powinien być mechanizm umożliwiający weryfikację reakcji tych sygnatur na chroniony ruch sieciowy***.".

Pytanie 25
W wymaganiu 22.5 dla NGFW (str. 11 pdf) Zamawiający definiuje wymaganie: „22.5 Musi być możliwość sprawdzenia wpływu na chroniony ruch sieciowy nowych sygnatur IPS bez konieczności ich zatwierdzenia na NGFW."
Wymaganie to stanowi cechę szczególną rozwiązania Cisco. Producenci w różny sposób realizują proces aktualizacji sygnatur i innych elementów bezpieczeństwa systemów NGFW. Z tego względu prosimy o usunięcie punktu 22.5 jako zapisu ograniczającego konkurencję.

ODPOWIEDŹ:
Zamawiający udzielił odpowiedzi na to pytanie w odpowiedzi na pytanie nr 24 powyżej.

Pytanie 26
W punkcie 19.10 „Zasady oceny kryterium „Dodatkowa funkcjonalność" (DF) w zakresie części 4" Zamawiający opisuje dodatkowo punktowane funkcjonalności. W trzech pierwszych punktach mamy:
Zgodność NGFW z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub równoważnym. (5 pkt.)
Zgodność NGFW i Konsoli Zarządzającej z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile for Network Devices v2.1" lub równoważnym. (24 pkt.)
Zgodność NGFW z profilem zabezpieczeń Common Criteria – „PP-Module for Virtual Private Network (VPN) Gateways" lub równoważnym. (5 pkt).

Proces certyfikacji Common Criteria jest procesem długotrwałym (zazwyczaj trwa od 9 do 18 miesięcy od wyprodukowania nowej wersji oprogramowania lub nowej wersji urządzenia. W certyfikatach umieszczonych na stronie Common Criteria przedstawiany jest model urządzenia oraz wersja oprogramowania dla których uzyskany został certyfikat. W każdym przypadku oznacza to, że wersje oprogramowania uwzględnione w certyfikacie CC w chwili jego uzyskania będą posiadały nowe znane podatności oraz poprawki. Jedną z podstawowych zasad bezpieczeństwa jest aktualizowanie oprogramowanie, zwłaszcza w tak krytycznym miejscu jak urządzenia NGFW.
Czy zamawiający wymaga dostarczenia urządzeń posiadających certyfikat CC w wersji oprogramowania w wersji dokładnie jak na certyfikacie?
Czy też może zostać dostarczone urządzenie certyfikowane (zgodnie z certyfikatem CC) ale z zainstalowaną nowszą/najnowszą wersją oprogramowania?

ODPOWIEDŹ:

Zamawiający wymaga dostarczenia Urządzenia zgodnego z Ofertą Wykonawcy, z którym została zawarta umowa w sprawie zamówienia publicznego. Jeżeli zatem Wykonawca zaoferuje np. Urządzenie, posiadające cechę wskazaną jako kryterium oceny ofert, którą posiada Urządzenie wyłącznie w konkretnej wersji oprogramowania, to Wykonawca zobowiązany jest dostarczyć takie właśnie urządzenie – natomiast, Zamawiający wymaga dostarczenia Urządzenia wraz ze Wsparciem Technicznym, umożliwiającym upgrade i downgrade do dowolnej wspieranej przez producenta wersji oprogramowania – zgodnie z wymogiem zawartym w pkt III.4.(3) OPZ: „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". Poprzez kryterium wskazane w zadanym pytaniu, Zamawiający promuje zatem możliwość korzystania z urządzenia, objętego certyfikatem Common Criteria lub równoważnym.

Pytanie 27

W punkcie 9 OPZ NGFW „Wymagania dla urządzeń NGFW" Zamawiający określa:
„Każde z urządzeń musi być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej."
Biorąc pod uwagę wysokiej klasy wymagania Zamawiającego czy oferowane urządzenia NGFW oraz Konsola Zarządzania muszą posiadać możliwość pozostawienia dysków (nośnika) urządzenia u Zamawiającego i dokonywania procedury wymiany (RMA) bez zainstalowanych dysków (nośników)?
Czy Zamawiający wymaga możliwości samodzielnego niszczenia dysków (nośników) dla oferowanych urządzeń?

ODPOWIEDŹ:

Zgodnie z wymogami wskazanymi w pkt III.3.(3)(b) oraz III.3.(4) OPZ Zamawiający wymaga wykonywania napraw, wymagających odinstalowania urządzenia, wyłącznie „po trwałym usunięciu danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez Gwaranta i zdeponowaniu ich u Zamawiającego". Zatem musi być możliwość pozostawienia dysków (nośników) z urządzenia u Zamawiającego (z możliwością ich samodzielnego zniszczenia).

Pytanie 28

W punkcie 9 OPZ NGFW „Wymagania dla urządzeń NGFW" Zamawiający określa:
„Każde z urządzeń musi być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej."
Dla urządzeń Typ 1 i Typ 2 wymaganie na dwa dyski są uzasadnione.

Dla urządzenia Typ3 które charakteryzuje się bardzo małą przepustowością (1 Gbps) wymaganie redundantnych dysków powoduje konieczność zaoferowania bardzo drogich urządzeń dużej przepustowości tylko w celu spełnienia tego wymagania.
Dodatkowo zapis taki faworyzuje producenta Cisco, który posiada dwa dyski również w swoich wolniejszych urządzeniach.
Prosimy o usunięcie wymagania dla urządzeń Typ3.

ODPOWIEDŹ:

Zamawiający informuje, że dokonał zmiany postanowienia pkt III.1.2 pkt 9 w Rozdziale II – Opis przedmiotu zamówienia –część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, w następującym zakresie:
Przed zmianą:
„Każde z urządzeń musi być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej.”
Po zmianie:
„9.1 Każde z NGFW typ 1 i każde z NGFW typ 2 musi być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej.
9.2 Każde z NGFW typu 3 powinno być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej*.”.

Pytanie 29

15.12 Musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.	Czy Zamawiający zgodzi się na wykrywanie aktywności sieci typu Botnet na podstawie informacji z Threat Intelligence Producenta?

ODPOWIEDŹ:

Zamawiający informuje, że dokonał zmiany postanowienia pkt III.1.2. ppkt 15.12 OPZ, w następującym zakresie:
Przed zmianą:
„15.12 Musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.”
Po zmianie:
„15.12 Powinien posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej**.”

Pytanie 30

17 - Funkcjonalność VPN w **NGFW typu 2 i 3** 17.1 Musi posiadać funkcjonalność VPN typu clientless (SSL/TLS) oraz SSL VPN oraz zestawiania tuneli IPSEC.	Czy Zamawiający zgodzi się na dedykowane rozwiązanie realizujące funkcjonalność VPN clientless? Czy Zamawiający zgodzi się na usunięcie tego zapisu ze względu na ograniczenie konkurencji?

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na zmianę postanowienia wskazanego w pytaniu. Zamawiający zgadza się na dedykowane (min. dwa fizyczne - w celu zachowania redundancji) rozwiązania realizujące funkcjonalność VPN clientless, opisaną w III.1.2. ppkt 17.1. w Rozdziale II - Opis przedmiotu zamówienia

- część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją.

Pytanie 31

17.4 Ilość wspieranych równoległych tuneli VPN typu clientless nie mniejsza niż 100.	Czy Zamawiający zgodzi się na dedykowane rozwiązanie realizujące funkcjonalność VPN clientless? Czy Zamawiający zgodzi się na usunięcie tego zapisu ze względu na ograniczenie konkurencji?

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na zmianę postanowienia wskazanego w pytaniu. Zamawiający zgadza się na dedykowane rozwiązanie realizujące funkcjonalność opisaną w III.1.2. ppkt 17.4. w Rozdziale II - Opis przedmiotu zamówienia - część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją.

Pytanie 32

III.1.1 Wymagania ogólne dla Urządzeń:
Czy Zamawiający podtrzymuje wymóg redundancji zasilania typu hot-plug dla NGFW – typ 3

ODPOWIEDŹ:

Zamawiający podtrzymuje wymóg redundancji zasilania typu hot-plug dla NGFW – typ 3.

Pytanie 33

dot. 6.4.1. III.1.2 Wymagania dla urządzeń NGFW.
Prosimy o potwierdzenie, że Zamawiający wymaga dostarczenia z każdym z urządzeń zarówno 8 szt. wkładek SFP typu SX jak i 8 sztuk 1000Base-T przy podtrzymaniu war. 6.3 i że wkładki te mają być dostarczone nawet jeśli sumaryczna ich ilość jest większa niż ilość slotów SFP/SFP+ dostępna na urządzeniu NGFW typ 2 przewidziana do osadzenia wymiennych wkładek ?

ODPOWIEDŹ:

Zamawiający potwierdza, że wymaga dostarczenia z każdym z urządzeń typu 2 zarówno 8 szt. wkładek SFP typu SX jak i 8 sztuk 1000Base-T przy podtrzymaniu war. 6.3 i że wkładki te mają być dostarczone nawet jeśli sumaryczna ich ilość jest większa niż ilość slotów SFP/SFP+ dostępna na urządzeniu NGFW typ 2 przewidziana do osadzenia wymiennych wkładek.

Pytanie 34

dot. 6.6.1. III.1.2 Wymagania dla urządzeń NGFW.
Prosimy o potwierdzenie, że Zamawiający wymaga dostarczenia z każdym z urządzeń zarówno 8 szt. wkładek SFP typu SX jak i 8 sztuk 1000Base-T i że w/w wkładki mają być dostarczone nawet jeśli sumaryczna ich ilość jest większa niż ilość slotów SFP dostępna na urządzeniu NGFW typ 3 ?

ODPOWIEDŹ:

Zamawiający potwierdza, że wymaga dostarczenia z każdym z urządzeń typu 3 zarówno 8 szt. wkładek SFP typu SX jak i 8 sztuk 1000Base-T i że w/w wkładki mają być dostarczone nawet jeśli sumaryczna ich ilość jest większa niż ilość slotów SFP dostępna na urządzeniu NGFW typ 3.

Pytanie 35
dot. 7. 1.2 Wymagania dla urządzeń NGFW.
Czy urządzenia (dla każdego z typów NGFW 1 2 i 3) mają być zalicencjonowane do pracy w trybie klastra i użycia mechanizmu HA z jednoczesnym brakiem możliwości pracy jako urządzenia całkowicie od siebie niezależne (nie działające w klastrze/HA), czy mają być dostarczone z licencją umożliwiającą działanie urządzeń jako całkowicie niezależne lub w klastrze (ten model licencjonowania może być kosztowniejszy z punktu widzenia zamawiającego)?

ODPOWIEDŹ:
Zamawiający wyjaśnia, że każde z NGFW typ 1, typ 2 i typ 3 musi mieć możliwość działania (w ramach typu NGFW):

- niezależnie,
- w klastrze,
- w HA.

Pytanie 36
III.1.2 Wymagania dla urządzeń NGFW.
Czy Zamawiający podtrzymuje wymóg redundancji dysków również dla NGFW – typ 3 ?

ODPOWIEDŹ:
Zamawiający udzielił odpowiedzi na to pytanie w odpowiedzi na pytanie nr 28 powyżej.

Pytanie 37
III.1.2 Wymagania dla urządzeń NGFW.
Prosimy o potwierdzenie, że Zamawiający wymaga wsparcia na każdym z typów NGFW (typ 1,2 i 3) funkcjonalności VPN typu clientless i zgodnie z wym. 17.4 dla co najmniej 100 jednoczesnych tuneli na każdym z typów NGFW

ODPOWIEDŹ:
Zamawiający wymaga wsparcia funkcjonalności VPN typu clientless dla co najmniej 100 jednoczesnych tuneli - na każdym z NGFW **typ 2** i na każdym NGFW **typ 3**- zgodnie z pkt 17 OPZ wiersz „Funkcjonalność VPN w **NGFW typu 2 i 3**".

Pytanie 38
III.1.2 Wymagania dla urządzeń NGFW.
Czy Zamawiający wymaga dostarczenia wraz z urządzeniami NGFW któregokolwiek z typów (Typ 1, 2 3) licencji/subskrypcji zapewniających ochronę przez zagrożeniami tzw. "dnia-zerowego" (sandboxing)?

ODPOWIEDŹ:
Zamawiający potwierdza, że nie wymaga dostarczenia wraz z urządzeniami NGFW któregokolwiek z typów (Typ 1, 2 3) licencji/subskrypcji zapewniających ochronę przez zagrożeniami tzw. "dnia-zerowego" (sandboxing).

Pytanie 39
III.2 Zasady realizowania Godzin eksperckich w ramach prawa opcji .
Prosimy o wyjaśnienie co Zamawiający rozumie pod pojęciem: "autoryzowany podmiot współpracujący z producentem przedmiotu zamówienia ..". Czy Zamawiający ma na myśli oferenta (integratora) o ile ten spełnia wymaganie dot. poziomu partnerstwa : "w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, o nie

więcej niż jeden stopień" , czy chodzi o podmiot będący wyłącznie dystrybutorem producenta oferowanego rozwiązania NGFW w teorii zdolny do realizacji takich usług wsparcia ?

ODPOWIEDŹ:

Zamawiający, w cytowanym postanowieniu definiuje wymaganie, aby poszczególne świadczenia, realizowane na podstawie umowy w sprawie zamówienia publicznego były wykonywane przez podmiot autoryzowany, współpracujący z producentem przedmiotu zamówienia. Zgodnie z definicją zawartą w Słowniku Języka Polskiego, „autoryzacja", w kontekście cytowanego wyżej wymogu oznacza „zezwolenie producenta na prowadzenie działalności w jego imieniu". Zamawiający wymaga zatem, aby podmiot spełniający dane świadczenie współpracował z producentem dostarczonego rozwiązania, występował w jego imieniu jako partner biznesowy **„**w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, o nie więcej niż jeden stopień". Zamawiający, przewidując możliwość zakupu towarów i usług pochodzących od różnych producentów, budujących sieci dystrybucyjne w różny sposób i stosując różne podziały partnerów według obszarów tematycznych, kompetencji, geograficznych obszarów aktywności biznesowej czy wolumenów dostaw – nie formułuje wymagań w tym zakresie, wymagając jednocześnie realizowania świadczeń bezpośrednio przez producenta dostarczanego rozwiązania lub podmiot współpracujący z takim producentem we wskazanym przez Zamawiającego zakresie. Zamawiający ocenia bowiem, że takie elementy świadczenia jak np. zapewnienie dostępu do aktualizacji tzw. firmware, mogą być spełniane bezpośrednio przez producenta takiego oprogramowania lub jego partnera, nie będącego bezpośrednim kontrahentem Zamawiającego.

Pytanie 40

ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI IV

III.2 Zasady realizowania Godzin eksperckich w ramach prawa opcji pkt. 3 (e) . Prosimy o usunięcie wymagania posiadania certyfikatu potwierdzającego ukończenie szkolenia o jakim pisze Zamawiający w niniejszym punkcie. Inżynierowie oferenta świadczący usługę wsparcia eksperckiego mają bowiem spełniać wymagania opisane w pkt. (1) i (2) co w pełni potwierdza ich kwalifikacje do wykonywania usług wsparcia z obszaru oferowanej technologii NGFW (wszelkich obszarów). Szkolenia o których pisze Zamawiający są szkoleniami przewidzianymi dla uczestnika końcowego (klienta) i certyfikowani inżynierowie nie uczestniczą w takich kursach gdyż ani nie podnoszą one poziomu ich wiedzy (potwierdzonego posiadaniem certyfikatów producenta) będąc tylko zbędnym kosztem.

ODPOWIEDŹ:

Zamawiający nie wyraża zgody na proponowaną zmianę SWZ.

Jednocześnie, na podstawie art. 137 ust. 1 ustawy Pzp, Zamawiający zmienia treść SWZ w zakresie części 3: Rozbudowa systemu IBM Qradar poprzez dostawę sprzętu i licencji wraz z usługami wsparcia technicznego i gwarancją oraz w zakresie części 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, tj.:

I W Rozdziale I - Instrukcja dla Wykonawców, Zamawiający wprowadza następujące zmiany:

I.1 Postanowienie 5.4 ppkt 1 otrzymuje następującą treść: „Maksymalny czas dostawy Sprzętu wraz z dokumentacją do 7 tygodni od dnia podpisania Umowy.".

I.2 Postanowienie pkt 19.10 „Zasady oceny kryterium „Dodatkowa funkcjonalność" (DF) w zakresie części 4:" otrzymuje następującą treść:

19.10. Zasady oceny kryterium „Dodatkowa funkcjonalność" (DF) w zakresie części 4:

19.10.1. W przypadku kryterium „Dodatkowe funkcjonalności" (DF) Wykonawca otrzyma następującą liczbę punktów:

Nazwa kryterium	**Punktacja**
Zgodność NGFW z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub równoważnym.	5 pkt
Zgodność NGFW i Konsoli Zarządzającej z profilem zabezpieczeń Common Criteria – "collaborative Protection Profile for Network Devices v2.1" lub równoważnym.	20 pkt
Zgodność NGFW z profilem zabezpieczeń Common Criteria – „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0 lub równoważnym.	5 pkt
NGFW posiada „Virtual patching" – ochronę umożliwiającą wdrażanie poprawek wirtualnych przed próbami wykorzystania podatności w chronionych systemach i aplikacjach.	1 pkt
NGFW umożliwia weryfikację zapytań DNS w celu wykrywania potencjalnego wycieku danych (exfiltracja danych do Internetu).	2 pkt
NGFW wspiera mechanizm pojedynczego logowania SSO (ang. Single Sign-On).	2 pkt
NGFW posiada możliwość deszyfracji ruchu (co najmniej TLS/SSL w oparciu o zaimportowanie klucza prywatnego) w celu jego analizy oraz szyfracji ruchu z powrotem.	1 pkt
NGFW typu 3 jest wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej.	1 pkt
NGFW posiada funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.	2 pkt
NGFW posiada możliwość sprawdzenia wpływu na chroniony ruch sieciowy nowych sygnatur IPS bez konieczności ich zatwierdzenia na NGFW, tzn. przed włączeniem nowych sygnatur IPS z trybem blokowania powinien być mechanizm umożliwiający weryfikację reakcji tych sygnatur na chroniony ruch sieciowy	1 pkt

19.10.2. Zasady oceny podkryterium „Zgodność NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub równoważnym":

1) Zamawiający **przyzna punkty** w kryterium „Zgodność NGFW z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub równoważnym" Wykonawcy, który zaoferuje NGFW o funkcjonowaniu zgodnym z profilem „collaborative Protection Profile for Stateful Traffic Filter Firewalls v1.3" wymienione na stronie internetowej https://www.commoncriteriaportal.org/products/#NS, w sposób potwierdzający:
   a. zgodność oferowanego urządzenia z „collaborative Protection Profile for Stateful Traffic Filter Firewalls v1.3" lub wersją nowszą,
   b. dowolny stopień zgodności (np. „PP Compliant", EAL1 lub wyżej),

2) Zamawiający **nie przyzna punktów** w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę NGFW, wskazane w formularzu ofertowym będą zawarte na innej liście opublikowanej w domenie commoncriteria.org, w szczególności nie przyzna punktów Wykonawcom oferującym NGFW wymienione na stronie internetowej https://www.commoncriteriaportal.org/products/index.cfm?archived=1;
3) Zamawiający **nie przyzna punktów** w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę NGFW, wskazane w formularzu ofertowym będą zawarte na jakiejkolwiek liście opublikowanej w domenie commoncriteria.org, wskazującej na ich zgodność z inną wersją profilu Common Criteria niż wskazana przez Zamawiającego w opisie niniejszego kryterium wersja: „collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.3" lub wersją nowszą;
4) Zamawiający przyzna punkty niezależnie od posiadania przez oferowane NGFW zgodności z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices v2.1" lub równoważnym albo „PP-Module for Virtual Private Network (VPN) Gateways " w wersji 1.0 lub równoważnym, stanowiących przedmiot odrębnych kryteriów oceny ofert.

19.10.3. Zamawiający wskazuje następujące warunki równoważności dla systemu równoważnego dla Common Criteria:
1) System opracowany na podstawie porozumienia podmiotów prawa publicznego, utworzonych w celu realizowania zadań związanych z informatyzacją, z co najmniej 10 krajów w tym co najmniej 5 Państw Członkowskich Unii Europejskiej lub NATO;
2) System i funkcjonuje co najmniej od 10 lat;
3) System obejmuje powoływanie niezależnych podmiotów certyfikujących, wykonujących oceny zgodnie z metodologią przyjętą w ramach tego systemu;
4) System zawiera metodologię ewaluacji i tworzenia wzorców normatywnych zabezpieczeń sprzętu oraz opracowane wzorce dla sprzętów sieciowych oraz sprzętów typu Firewall;
5) System musi obejmować szczegółowe wymagania co najmniej w następujących obszarach: komunikacja z urządzeniami sieciowymi, aktualizacje, aktywność na potrzeby audytu, wymiana danych uwierzytelniających, błędy urządzeń, ochrona fizyczna, polityka bezpieczeństwa, zarządzanie kluczami kryptograficznymi, operacje kryptograficzne, generator liczb losowych, ochrona informacji, identyfikacja
i autoryzacja, zarządzanie hasłami, identyfikacja użytkownika, zarządzanie bezpieczeństwem, ochrona kluczowych danych, monitorowanie dostępu;
6) System powinien być ogólnie dostępny, możliwy do zweryfikowania przez Zamawiającego;
7) System został wskazany 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;
8) Zamawiający uzna jako równoważny system obejmujący zgodność z innym profilem ustanowionym w ramach porozumienia o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA, pod warunkiem, że wykonawca w załączonym dokumencie wykaże brak sprzeczności pomiędzy tym profilem oraz profilem „collaborative Protection Profile for Network Devices v2.1 " i „PP-Module for Virtual Private Network (VPN) Gateways" w wersji

1.0, a także przedmiotowo istotne różnice pomiędzy profilami, uzasadniające twierdzenie, że profile te nie są sprzeczne, w kontekście wszystkich funkcjonalności oferowanego urządzenia;

9) Zamawiający nie uznaje wcześniejszych wersji profilu zabezpieczeń Common Criteria za równoważne wersjom wskazanym przez Zamawiającego w opisie niniejszego podkryterium.

19.10.4. Zasady oceny podkryterium „Zgodność NGFW i Konsoli Zarządzającej z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices v2.1" lub równoważnym:

1) Zamawiający przyzna punkty w kryterium „Zgodność NGFW i Konsoli Zarządzającej z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Network Devices v2.1" lub równoważnym" Wykonawcy, który zaoferuje NGFW i Konsolę Zarządzającą o funkcjonowaniu zgodnym z profilem „collaborative Protection Profile for Network Devices v2.1" wymienione na stronie internetowej https://www.commoncriteriaportal.org/products/#NS, w sposób potwierdzający:
   a. zgodność oferowanych urządzeń z „collaborative Protection Profile for Network Devices v2.1" lub wersją nowszą,
   b. dowolny stopień zgodności (np. „PP Compliant", EAL1 lub wyżej),
2) Zamawiający **nie przyzna punktów** w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę NGFW i Konsola Zarządzająca, wskazane w formularzu ofertowym będą zawarte na innej liście opublikowanej w domenie commoncriteria.org, w szczególności **nie przyzna punktów** Wykonawcom oferującym NGFW i Konsolę Zarządzającą wymienione na stronie internetowej https://www.commoncriteriaportal.org/products/index.cfm?archived=1 ;
3) Zamawiający **nie przyzna punktów** w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę NGFW, wskazane w formularzu ofertowym będą zawarte na jakiejkolwiek liście opublikowanej w domenie commoncriteria.org, wskazującej na ich zgodność z inną wersją profilu Common Criteria niż wskazana przez Zamawiającego w opisie niniejszego kryterium wersja: „collaborative Protection Profile for Network Devices v2.1" lub wersją nowszą
4) Zamawiający przyzna punkty niezależnie od posiadania przez oferowane NGFW i Konsoli Zarządzającej zgodności z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls v1.3" lub równoważnym albo „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0 lub równoważnym, stanowiących przedmiot odrębnych kryteriów oceny ofert.

19.10.5. Zamawiający wskazuje następujące warunki równoważności dla systemu równoważnego dla Common Criteria:

1) System opracowany na podstawie porozumienia podmiotów prawa publicznego, utworzonych w celu realizowania zadań związanych z informatyzacją, z co najmniej 10 krajów w tym co najmniej 5 Państw Członkowskich Unii Europejskiej lub NATO;
2) System funkcjonuje co najmniej od 10 lat;
3) System obejmuje powoływanie niezależnych podmiotów certyfikujących, wykonujących oceny zgodnie z metodologią przyjętą w ramach tego systemu;
4) System zawiera metodologię ewaluacji i tworzenia wzorców normatywnych zabezpieczeń sprzętu oraz opracowane wzorce dla sprzętów sieciowych oraz sprzętów typu Firewall;

5) System musi obejmować szczegółowe wymagania co najmniej w następujących obszarach: komunikacja z urządzeniami sieciowymi, aktualizacje, aktywność na potrzeby audytu, wymiana danych uwierzytelniających, błędy urządzeń, ochrona fizyczna, polityka bezpieczeństwa, zarządzanie kluczami kryptograficznymi, operacje kryptograficzne, generator liczb losowych, ochrona informacji, identyfikacja i autoryzacja, zarządzanie hasłami, identyfikacja użytkownika, zarządzanie bezpieczeństwem, ochrona kluczowych danych, monitorowanie dostępu;
6) System powinien być ogólnie dostępny, możliwy do zweryfikowania przez Zamawiającego;
7) System został wskazany 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;
8) Zamawiający uzna jako równoważny system obejmujący zgodność z innym profilem ustanowionym w ramach porozumienia o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA, pod warunkiem, że wykonawca w załączonym dokumencie wykaże brak sprzeczności pomiędzy tym profilem oraz profilem „collaborative Protection Profile for Stateful Traffic Filter Firewalls v1.3" i „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0, a także przedmiotowo istotne różnice pomiędzy profilami, uzasadniające twierdzenie, że profile te nie są sprzeczne, w kontekście wszystkich funkcjonalności oferowanego urządzenia;
9) Zamawiający nie uznaje wcześniejszych wersji profilu zabezpieczeń Common Criteria za równoważne wersjom wskazanym przez Zamawiającego w opisie niniejszego podkryterium.

19.10.6. Zasady oceny podkryterium „Zgodność NGFW z profilem zabezpieczeń Common Criteria – „PP-Module for Virtual Private Network (VPN) Gateways" w wersji v1.0 lub równoważnym":

1) Zamawiający przyzna punkty w kryterium „Zgodność NGFW z profilem zabezpieczeń Common Criteria – „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0 lub równoważnym" Wykonawcy, który zaoferuje NGFW o funkcjonowaniu zgodnym z profilem „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0 wymienione na stronie internetowej https://www.commoncriteriaportal.org/products/#NS w sposób potwierdzający:
   a. zgodność oferowanego urządzenia z „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0 lub wersji nowszej,
   b. dowolny stopień zgodności (np. „PP Compliant", EAL1 lub wyżej),
2) Zamawiający **nie przyzna punktów** w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę NGFW, wskazane w formularzu ofertowym będą zawarte na innej liście opublikowanej w domenie commoncriteria.org, w szczególności **nie przyzna punktów** Wykonawcom oferującym NGFW wymienione na stronie internetowej https://www.commoncriteriaportal.org/products/index.cfm?archived=1 ;
3) Zamawiający **nie przyzna punktów** w tym kryterium oceny ofert, jeżeli oferowane przez Wykonawcę NGFW, wskazane w formularzu ofertowym będą zawarte na jakiejkolwiek liście opublikowanej w domenie commoncriteria.org, wskazującej na ich zgodność z inną wersją profilu Common Criteria niż wskazana przez

Zamawiającego w opisie niniejszego kryterium wersja: „PP-Module for Virtual Private Network (VPN) Gateways" w wersji 1.0 lub wersja nowsza;

4) Zamawiający przyzna punkty niezależnie od posiadania przez oferowane NGFW zgodności z profilem zabezpieczeń Common Criteria – „collaborative Protection Profile for Stateful Traffic Filter Firewalls v1.3" lub równoważnym albo „collaborative Protection Profile for Network Devices v2.1" lub równoważnym, stanowiących przedmiot odrębnych kryteriów oceny ofert.

19.10.7. Zamawiający wskazuje następujące warunki równoważności dla systemu równoważnego dla Common Criteria:

1) System opracowany na podstawie porozumienia podmiotów prawa publicznego, utworzonych w celu realizowania zadań związanych z informatyzacją, z co najmniej 10 krajów w tym co najmniej 5 Państw Członkowskich Unii Europejskiej lub NATO;
2) System funkcjonuje co najmniej od 10 lat;
3) System obejmuje powoływanie niezależnych podmiotów certyfikujących, wykonujących oceny zgodnie z metodologią przyjętą w ramach tego systemu;
4) System zawiera metodologię ewaluacji i tworzenia wzorców normatywnych zabezpieczeń sprzętu oraz opracowane wzorce dla sprzętów sieciowych oraz sprzętów typu Firewall;
5) System musi obejmować szczegółowe wymagania co najmniej w następujących obszarach: komunikacja z urządzeniami sieciowymi, aktualizacje, aktywność na potrzeby audytu, wymiana danych uwierzytelniających, błędy urządzeń, ochrona fizyczna, polityka bezpieczeństwa, zarządzanie kluczami kryptograficznymi, operacje kryptograficzne, generator liczb losowych, ochrona informacji, identyfikacja i autoryzacja, zarządzanie hasłami, identyfikacja użytkownika, zarządzanie bezpieczeństwem, ochrona kluczowych danych, monitorowanie dostępu;
6) System powinien być ogólnie dostępny, możliwy do zweryfikowania przez Zamawiającego;
7) System został wskazany 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;
8) Zamawiający uzna jako równoważny system obejmujący zgodność z innym profilem ustanowionym w ramach porozumienia o wzajemnym respektowaniu rezultatów oceny i certyfikacji bezpiecznych produktów informatycznych - CCRA, pod warunkiem, że wykonawca w załączonym dokumencie wykaże brak sprzeczności pomiędzy tym profilem oraz profilem „collaborative Protection Profile for Stateful Traffic Filter Firewalls v1.3" i „collaborative Protection Profile for Network Devices v2.1", a także przedmiotowo istotne różnice pomiędzy profilami, uzasadniające twierdzenie, że profile te nie są sprzeczne, w kontekście wszystkich funkcjonalności oferowanego urządzenia.
9) Zamawiający nie uznaje wcześniejszych wersji profilu zabezpieczeń Common Criteria za równoważne wersjom wskazanym przez Zamawiającego w opisie niniejszego podkryterium.

19.10.8. Maksymalna liczba punktów jakie może uzyskać Wykonawca w tym kryterium to 40 pkt."

II W Rozdziale II - Opis przedmiotu zamówienia - część 4: Dostawa urządzeń firewall (ang. Next

Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, Zamawiający wprowadza następujące zmiany:

II.1 Postanowienie III.1. ppkt (b) otrzymuje następującą treść: „dwóch konsol zarządzających w/w NGFW, zwanych dalej „**Konsolami Zarządzającymi**". zwanych łącznie „**Urządzeniami**", w terminie siedmiu tygodni od dnia podpisania umowy.".

II.2 postanowienie III.1.2. pkt 9 „Pamięć wewnętrzna na system operacyjny", ppkt - otrzymuje następującą treść: „9.1 Każde z NGFW typ 1 i każde z NGFW typ 2 musi być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej. 9.2 Każde z NGFW typu 3 powinno być wyposażone w co najmniej dwa dyski (na system operacyjny) w konfiguracji redundantnej[*]" z przypisem „[*]" o następującej treści w stopce dokumentu: „[*]Stanowi kryterium oceny ofert".

II.3 postanowienie III.1.2. pkt 15 „Funkcjonalność aktualizacji i ochrony NGFW", ppkt 15.12 otrzymuje następującą treść: „Powinien posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej[**]" z przypisem „[**]" o następującej treści w stopce dokumentu: „[**]Stanowi kryterium oceny ofert".

II.4 Postanowienie III.1.2. pkt 16 „Ochrona IPS - możliwe reakcje na wykryte zdarzenia bezpieczeństwa w przetwarzanym ruchu sieciowym" ppkt 16.4 otrzymuje następującą treść: „16.4 Dla wskazanych IP (podsieci) lub stref bezpieczeństwa musi być możliwość definiowania różnych reakcji (16.1-16.3) lub profili IPS oraz różnych konfiguracji polityk bezpieczeństwa.".

II.5 postanowienie III.1.3. pkt 22 „Wymagania funkcjonalne", ppkt 22.5 otrzymuje następującą treść: „Powinien być możliwość sprawdzenia wpływu na chroniony ruch sieciowy nowych sygnatur IPS bez konieczności ich zatwierdzenia na NGFW[***]" z przypisem „[***]" o następującej treści w stopce dokumentu: „[***]Stanowi kryterium oceny ofert".

III W Rozdziale III - Projektowane postanowienia umowy – część 3: Rozbudowa systemu IBM Qradar poprzez dostawę sprzętu i licencji wraz z usługami wsparcia technicznego i gwarancją, Zamawiający wprowadza następujące zmiany:

III.1 postanowienie § 1 wiersz 23 Tabeli otrzymuje następującą treść: „23. | Zlecenie | Dokument w formie pisemnej (w tym w formie elektronicznej, opatrzonej ważnym kwalifikowanym podpisem elektronicznym) - na podstawie którego Zamawiający zobowiązuje się powierzać Wykonawcy wykonywanie Godzin eksperckich, wskazujący zakres oraz terminy prac, których terminową realizację, jako Godzin eksperckich, zobowiązany jest zapewnić Wykonawca - sporządzony zgodnie ze wzorem, stanowiącym Załącznik nr 7 do Umowy.".

III.2 postanowienie § 5 ust. 6 otrzymuje następującą treść: „Po zakończeniu prac, zrealizowanych na podstawie Zlecenia, Strony zobowiązują się potwierdzić fakt ich wykonania w formie pisemnej (lub poprzez zastosowanie ważnego, kwalifikowanego podpisu elektronicznego), zgodnie ze wzorem stanowiącym Załącznik nr 8 do Umowy.".

III.3 postanowienie § 5 ust. 9 zd. 2 -4 otrzymuje następującą treść: „Niniejszy zakup jest dokonywany na rzecz klienta końcowego jakim będzie Skarb Państwa reprezentowany przez Ministra

Cyfryzacji. Wobec tego przedmiot zamówienia jest przeznaczony do jednorazowej dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę (klienta końcowego) jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji, ul. Królewska 27, 00-060 Warszawa.”.

IV W Rozdziale III - Projektowane postanowienia umowy – część 4: Dostawa urządzeń firewall (ang. Next Generation Firewall) oraz licencji wraz z usługami wsparcia technicznego i gwarancją, Zamawiający wprowadza następujące zmiany:

IV.1 postanowienie § 1 wiersz 7 Tabeli otrzymuje następującą treść: „23. | Zlecenie | Dokument w formie pisemnej (w tym w formie elektronicznej, opatrzonej ważnym kwalifikowanym podpisem elektronicznym) - na podstawie którego Zamawiający zobowiązuje się powierzać Wykonawcy wykonywanie Godzin eksperckich, wskazujący zakres oraz terminy prac, których terminową realizację, jako Godzin eksperckich, zobowiązany jest zapewnić Wykonawca - sporządzony zgodnie ze wzorem, stanowiącym Załącznik nr 7 do Umowy.”.

IV.2 postanowienie § 3 ust. 1 pkt 1) otrzymuje następującą treść: „Zobowiązuje się dostarczyć Sprzęt wraz z Dokumentacją do Lokalizacji w terminie 7 (siedmiu) tygodni od dnia zawarcia Umowy;”.

IV.3 postanowienie § 5 ust. 6 otrzymuje następującą treść: „Po zakończeniu prac, zrealizowanych na podstawie Zlecenia, Strony zobowiązują się potwierdzić fakt ich wykonania w formie pisemnej (lub poprzez zastosowanie ważnego, kwalifikowanego podpisu elektronicznego), zgodnie ze wzorem stanowiącym Załącznik nr 8 do Umowy”.

IV.4 postanowienie § 5 ust. 9 zd. 2 -4 otrzymuje następującą treść: „Niniejszy zakup jest dokonywany na rzecz klienta końcowego jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji. Wobec tego przedmiot zamówienia jest przeznaczony do jednorazowej dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę (klienta końcowego) jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji, ul. Królewska 27, 00-060 Warszawa.”.

V Zamawiający zmienia treść Rozdziału IV - Formularz Oferty wraz z załącznikami, nadając mu treść stanowiącą Załącznik nr 1 do niniejszego dokumentu.

W pozostałym zakresie zapisy SWZ pozostają bez zmian. Niniejsze odpowiedzi i zmiany stanowią integralną część SWZ.

Katarzyna Wasilewska
Dyrektor Generalny
/-/