Pytanie 1
Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga złożenia wraz z ofertą Świadectwa Bezpieczeństwa Przemysłowego.
Czy Zamawiający dopuści możliwość złożenia oferty przez Wykonawcę, który 2 sierpnia 2023 roku złożył wniosek o wydanie świadectwa bezpieczeństwa przemysłowego, o którym mowa w art. 56 Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. 2023, poz. 756, z późn. zm.), który posiada Pion Ochrony Informacji Niejawnych, a także który zatrudnia 4 osoby posiadające ważne poświadczenie bezpieczeństwa w zakresie dostępu do informacji niejawnych oznaczonych co najmniej klauzulą „tajne".

Zamawiający podtrzymuje warunek określony w punkcie 3.2 Zapytania Ofertowego, polegający na złożeniu wraz z ofertą Świadectwa Bezpieczeństwa Przemysłowego. Jednocześnie Zamawiający uznaje fakt złożenia przez Wykonawcę wniosku o wydanie Świadectwa Bezpieczeństwa Przemysłowego za niewystarczający.

Pytanie 2
Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga złożenia wraz z ofertą posiadanych i ważnych certyfikatów ISO 27001 dla świadczenia usług z zakresu cyberbezpieczeństwa, obejmujących swoim zakresem usługi SOC, ISO 9001, wystawionych przez podmiot certyfikujący akredytowany przez Polskie Centrum Akredytacji w zakresie normy, której dotyczy certyfikat.
Czy Zamawiający odstąpi od wymogu przedłożenia certyfikatów wystawionych przez podmiot certyfikujący akredytowany przez Polskie Centrum Akredytacji w zakresie normy, której dotyczy certyfikat?
Wymóg aby certyfikaty wystawione były przez podmioty certyfikujące akredytowane przez Polskie Centrum Akredytacji w zakresie normy, której dotyczy certyfikat w znaczący sposób ogranicza uczciwą konkurencję, a zgodnie z § 8 ust 4. Regulaminu „Przeprowadzenie badania rynku (…) wymaga stosowania zasad uczciwej konkurencji i równego traktowania wykonawców". Ust. 1 art. 16 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. 2023r., poz. 1605, z późn. zm.) również wskazuje, iż Zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie Wykonawców.
Tu wskazać należy, iż postawiony przez Zamawiającego wymóg nie wynika z Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwa (Dz.U. z 2019 r. poz. 2479, z późn. zm.) (dalej: Rozporządzenie) w którym określono jedynie, iż „podmiot świadczący usługi z zakresu cyberbezpieczeństwa jest obowiązany (…) posiadać, utrzymywać i aktualizować system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001 w zakresie obejmującym co najmniej świadczone usługi".
Rola, jaką odgrywa akredytacja w ekonomicznej infrastrukturze UE i EFTA znalazła odzwierciedlenie w Rozporządzeniu Parlamentu Europejskiego i Rady (WE) Nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U.UE.L.2008.218.30), ustanawiającym ramy prawne dla akredytacji w Europie. Rozporządzenie to zawiera m.in. postanowienia dotyczące uznawania certyfikatów i raportów wydawanych przez akredytowane jednostki oceniające zgodność.
Jednocześnie wskazać należy, iż wymóg aby certyfikaty wystawione były przez podmioty certyfikujące akredytowane przez **Polskie** Centrum Akredytacji dyskryminuje pozostałe jednostki akredytujące, które oficjalnie zostały wskazane przez rządy poszczególnych państw do oceny organizacji świadczących usługi w zakresie certyfikacji, weryfikacji, inspekcji, badań i wzorcowań (określanych jako usługi oceny zgodności), które są zrzeszone w European co-operation for Accreditation (EA). EA zostało uznane przez Komisję Europejską jako europejska infrastruktura

akredytacyjna, odpowiedzialna za harmonizację akredytacji na terenie Europy, w celu ułatwienia swobodnego międzynarodowego przepływu towarów i usług, zapewnienia bezpieczeństwa oraz ochrony zdrowia i środowiska. EA jako stowarzyszenie regionalne jest członkiem: International Laboratory Accreditation Cooperation (ILAC) oraz International Accreditation Forum (IAF).

Zamawiający nie odstępuje od wymogu przedłożenia certyfikatów wystawionych przez podmiot certyfikujący akredytowany przez Polskie Centrum Akredytacji w zakresie normy, której dotyczy certyfikat, przedstawionego w punkcie 3.1 Zapytania Ofertowego.

Pytanie 3

Wykonawca wskazuje, iż często utrata poufności następuje na skutek wykorzystania elektromagnetycznej emisji ujawniającej, pochodzącej z urządzeń teleinformatycznych, a utrata dostępności następuje w szczególności na skutek zakłócenia prac urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy. W związku z powyższym istotnym jest zapewnienie ochrony elektromagnetycznej systemu teleinformatycznego, która polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w tych systemach. Jak podnosi komentarz do art. 50 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnej (t.j. Dz.U. z 2023r., poz. 756, z późn. zm.) „Ochrona elektromagnetyczna systemu teleinformatycznego polega na niedopuszczeniu do utraty poufności i dostępności informacji niejawnych przetwarzanych w tych systemach. Utrata poufności następuje zwłaszcza na skutek wykorzystania elektromagnetycznej emisji ujawniającej, pochodzącej z urządzeń teleinformatycznych. Utrata dostępności następuje w szczególności na skutek zakłócenia prac urządzeń teleinformatycznych za pomocą impulsów elektromagnetycznych o dużej mocy. Ochronę elektromagnetyczną systemu zapewnia się w szczególności przez umieszczenie urządzeń teleinformatycznych, połączeń i linii we właściwych strefach bezpieczeństwa emisji lub przez zastosowanie urządzeń teleinformatycznych o obniżonym poziomie emisji lub ich ekranowanie z jednoczesnym filtrowaniem zewnętrznych linii zasilających i sygnałowych. Mówimy tu o trójwymiarowej przestrzeni otaczającej element aktywny systemu teleinformatycznego wykorzystywany do przetwarzania informacji niejawnych, wewnątrz którego infiltracja elektromagnetyczna jest praktycznie niemożliwa. Właściwe podmioty, przy zastosowaniu odpowiednich przedsięwzięć organizacyjno-proceduralnych, są w stanie zidentyfikować oraz wyeliminować potencjalne drogi ulotu emisji ujawniającej. Powiększenie rozmiaru strefy bezpieczeństwa emisji może przyczynić się do umożliwienia obniżenia wymagań w zakresie technicznego poziomu zabezpieczenia wykorzystywanych elementów aktywnych. Strefa ta może pokrywać się np. ze strefą nadzorowaną."

Wobec powyższego, czy w celu zapewnienia bezpieczeństwa informacji Zamawiający wymaga przedstawienia potwierdzenia, iż usługa realizowana będzie w centrum danych zapewniającym ochronę elektromagnetyczną systemu teleinformatycznego, tj. przedłożenia Certyfikatu Ochrony Elektromagnetycznej, o którym mowa w ust. 5 art. 50 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnej, wystawionego przez ABW lub SKW?

Zamawiający nie wymaga przedłożenia Certyfikatu Ochrony Elektromagnetycznej, o którym mowa w ust. 5 art. 50 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnej, wystawionego przez ABW lub SKW. Zamawiający w punkcie 3.5 Zapytania Ofertowego wymaga, aby wszystkie obiekty, w których będzie świadczona usługa spełniały wymagania ujęte w Rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu czyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

Pytanie 4
Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga, aby **wybrany w toku postępowania Wykonawca** przedstawił posiadane przez zatrudnionych na umowę o pracę analityków bezpieczeństwa certyfikaty: CEH, Comptia Security+.
W związku z użytym sformułowaniem „wybrany w toku postępowania Wykonawca" Wykonawca zwraca się z wnioskiem o potwierdzenie, iż rzeczone certyfikaty należy złożyć dopiero w odpowiedzi na wezwanie Zamawiającego nie zaś na etapie składania ofert.

Posiadane przez zatrudnionych na podstawie umowy o pracę analityków bezpieczeństwa, o których mowa w punkcie 3.3 Zapytania Ofertowego, certyfikatów CEH, CompTia Security+ muszą być przedstawione wraz z ofertą, o czym mówi punkt 3.4 Zapytania Ofertowego.

Pytanie 5
Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga, aby wybrany w toku postępowania Wykonawca przedstawił posiadane przez zatrudnionych na umowę o pracę analityków bezpieczeństwa certyfikaty: CEH, Comptia Security+. **Czy Zamawiający uzna spełnienie wymogu jeżeli wybrany w toku postępowania Wykonawca przedstawi posiadane przez osoby skierowane do realizacji przedmiotu zamówienia certyfikaty, a mianowicie CEH oraz Comptia Security+ lub Microsoft SC-900 lub Cisco Introduction to cybersecurity lub C)IHE: Certified Incident Handling Engineer lub Audytor Wiodący ISO 27001?**

Zamawiający podtrzymuje wymóg przedstawienia certyfikatów CEH i/lub CompTia Security+ posiadanych przez wszystkich analityków bezpieczeństwa, o których mowa w punkcie 3.3. Zapytania Ofertowego, przy czym obowiązek posiadania co najmniej jednego wymaganego certyfikatu dotyczy wszystkich analityków, a każdy z wymaganych certyfikatów powinien wystąpić co najmniej raz. Jednocześnie Zamawiający nie uzna za wystarczające przedstawienie innych certyfikatów.

Pytanie 6
Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga złożenia wraz z ofertą oświadczenia o zatrudnieniu na podstawie aktualnych umów o pracę na pełny etat minimum 8 analityków bezpieczeństwa. Umowy powinny obowiązywać co najmniej od pełnego miesiąca poprzedzającego miesiąc złożenia oferty. W dzisiejszych czasach fluktuacja pracowników jest zjawiskiem nader częstym, niemożliwym do uniknięcia. Z 53 "Monitora Rynku Pracy" przeprowadzonego przez Randstad we współpracy z Instytutem Badań Pollster wynika, że w ciągu 6 miesięcy poprzedzających badanie pracodawcę zmieniło 20 proc. zatrudnionych.
W związku z powyższym wnioskujemy o modyfikację warunków udziału w sposób następujący:
„Oświadczenia o skierowaniu do realizacji zadania minimum 8 analityków bezpieczeństwa, w tym zatrudnieniu na podstawie aktualnych umów o pracę na pełny etat minimum 7 8 analityków bezpieczeństwa. Umowy powinny obowiązywać co najmniej od pełnego miesiąca poprzedzającego miesiąc złożenia oferty. (…)"

Zamawiający nie wyraża zgody na zmianę wymogu przedstawionego w punkcie 3.3 Zapytania Ofertowego.

Pytanie 7
Na potwierdzenie spełniania warunków udziału w postępowaniu Zamawiający wymaga, aby wybrany w toku postępowania Wykonawca przedstawił co najmniej dwie referencje na świadczenie usługi SOC z wykorzystaniem systemu SIEM Wykonawcy wystawionych przez podmioty kwalifikowane jako Operatorzy Usług Kluczowych na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, lub placówek Służby Zdrowia posiadających w swoich strukturach Oddział Intensywnej Opieki Medycznej lub Specjalistyczny Oddział Ratunkowy, na rzecz których usługa była świadczona przez Wykonawcę w ciągu ostatniego roku, przy czym wartość

świadczenia usługi powinna być nie mniejsza niż 350.000 zł brutto. Wykonawca wskazuje, iż większość umów, których przedmiotem jest świadczenie usługi SOC z wykorzystaniem systemu SIEM Wykonawcy, jest zawieranych na okres 12 m-cy, a wartość roczna umowy wynosi około 100 000,00 złotych brutto.

Wykonawca zwraca się z wnioskiem o modyfikację ww. wymogu w sposób następujący:

„Co najmniej dwóch referencji na świadczenie usługi SOC z wykorzystaniem systemu SIEM Wykonawcy wystawionych przez podmioty kwalifikowane jako Operatorzy Usług Kluczowych na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, lub podmiotem leczniczym w rozumieniu Ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz. U 2023, poz. 991, z późn. zm.) prowadzącym działalność leczniczą, o której mowa w art. 8 pkt 1 lit. a placówek Służby Zdrowia posiadających w swoich strukturach Oddział Intensywnej Opieki Medycznej lub Specjalistyczny Oddział Ratunkowy, na rzecz których usługa była świadczona przez Wykonawcę w ciągu ostatniego roku, przy czym roczna wartość przedmiotu umowy powinna być nie mniejsza niż 100.000 zł brutto, przy czym wartość świadczenia usługi powinna być nie mniejsza niż 350.000 zł brutto."

Zamawiający nie wyraża zgody na proponowaną zmianę brzmienia punktu 3.7 Zapytania Ofertowego. Jednocześnie Zamawiający zgadza się na obniżenie wartości świadczonej usługi do wartości nie mniejszej niż 100.000 zł rocznie. Zatem punkt 3.7 Zapytania Ofertowego otrzymuje brzmienie:

„Co najmniej dwóch referencji na świadczenie usługi SOC z wykorzystaniem systemu SIEM Wykonawcy wystawionych przez podmioty kwalifikowane jako Operatorzy Usług Kluczowych na podstawie ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa, lub placówek Służby Zdrowia posiadających w swoich strukturach Oddział Intensywnej Opieki Medycznej lub Specjalistyczny Oddział Ratunkowy, na rzecz których usługa była świadczona przez Wykonawcę w ciągu ostatniego roku, przy czym wartość świadczenia usługi powinna być nie mniejsza niż 100.000 zł brutto w skali roku."