MINISTERSTWO OBRONY NARODOWEJ
DEPARTAMENT ADMINISTRACYJNY

MINISTERSTWO OBRONY NARODOWEJ
WYDZIAŁ KANCELARII JAWNYCH
Nr. 2589/DA
24 CZE 2020
XLI XLI

Warszawa, dnia 24 czerwca 2020 r

Uczestnicy postępowania
o udzielenie zamówienia publicznego

Dotyczy: *postępowania o udzielenie zamówienia publicznego na usługę polegającą na przeprowadzeniu weryfikacji stanu aktualnego i sposobu osiągnięcia stanu docelowego w zakresie uzyskania informacji przestrzegania postanowień ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 ze zm.) przez podmioty lecznicze utworzone i nadzorowane przez Ministra Obrony Narodowej działające w formie samodzielnych publicznych zakładów opieki zdrowotnej i instytutów badawczych,* nr sprawy 15/ZP/20.

Szanowni Państwo,

Ministerstwo Obrony Narodowej jako Zamawiający w niniejszym postępowaniu o udzielenie zamówienia publicznego, działając zgodnie z art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843) przekazuje poniżej wyjaśnienia treści specyfikacji istotnych warunków zamówienia, zwanej dalej SIWZ:

Pytanie 1
Zamawiający sformułował wymagania dotyczące niezbędnego doświadczenia w następujący sposób:

- Wykonawca zrealizował co najmniej 2 projekty dotyczące wdrożenia wymagań norm ISO 27001 o wartości co najmniej 50,000 zł brutto w organizacjach zatrudniających co najmniej 100 pracowników.

- Wykonawca zrealizował co najmniej 2 projekty dotyczące wdrożenia wymagań norm ISO 223001 o wartości co najmniej 50,000 zł brutto w organizacjach zatrudniających co najmniej 100 pracowników.

Wyk. J.Gajewski - osobiście
T: 2612 B5

Wymagania tak sformułowane nie są tożsame z przedmiotem zamówienia, który dotyczy audytu systemu. Czy Zamawiający może dopuścić usługi audytu w w/w zakresie jako spełniające warunki postępowania?

Odpowiedź

Zamawiający na podstawie art. 121 ust 2 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2020 r., poz. 295) w ramach sprawowanego nadzoru zamierza uzyskać informację o stanie dostosowania podmiotów leczniczych działających w formie instytutu badawczego i samodzielnych publicznych zakładów opieki zdrowotnej będących operatorami usługi kluczowej do wymagań wynikających z postanowień ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 ze zm.), zwanej dalej ustawą.

Podmioty lecznicze utworzone i nadzorowane przez Ministra Obrony Narodowej działające w formie samodzielnych publicznych zakładów opieki zdrowotnej i instytutów badawczych świadczą usługi w sektorze ochrony zdrowia. Usługi te są uzależnione od bezpiecznego funkcjonowania systemów informacyjnych. Wystąpienie incydentów ma istotny skutek zakłócający dla świadczenia usługi kluczowej.

Zamawiający w Rozdziale III ust. 4 pkt 1 SIWZ wskazał: *Wymaga się, aby analiza i ocena realizowana była w oparciu o normę PN ISO/IEC 27001 oraz normę PN ISO/IEC 22301.*

Nieodzowne jest przytoczenie wyjaśnień czym są te dokumenty:

1. Międzynarodowa norma ISO / IEC 27001 stanowi: Technologię informacyjną - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji - Wymagania określające wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia udokumentowanego systemu zarządzania bezpieczeństwem informacji, z uwzględnieniem kontekstu organizacji. Obejmuje również wymagania dotyczące oceny i postępowania w przypadku zagrożeń bezpieczeństwa informacji zgodnie z indywidualnymi potrzebami organizacji. Przeznaczona jest do planowania, wdrażania, monitorowania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w organizacji (ISMS).
2. Międzynarodowa norma ISO 22301 Societal Security – Business Continuity Mangement Systems Requierements, rekomenduje zasady zarzadzania ciągłością działania.

Nie ulega wątpliwości, że obydwa te dokumenty wiążą się ściśle ze wzmocnieniem cyberbezpieczeństwa i związane są z ustawą. Stanowią standardy związane z zarzadzaniem bezpieczeństwem oraz zachowaniem ciągłości działania poszczególnych podmiotów leczniczych. Są więc ściśle związane z przedmiotem zamówienia.

Warto podkreślić, że wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji w organizacji, w tym przypadku w podmiotach leczniczych wiąże się właśnie z działaniami ujętymi w normie ISO / IEC 27001, między innymi związanymi z opracowaniem strategii w zakresie zarządzania ryzykiem.

Z powyższego zapisu wynika już uzasadnienie konieczności posiadania doświadczenia Wykonawcy ze stosowania wymagań zapisanych w przytoczonych dokumentach.

Ustawa odnosi się do tych dokumentów między innymi w art. 15, pkt 3. *Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, o której mowa w ust. 2 pkt 2 lit. b i c, uważa się udokumentowane wykonanie w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów w zakresie* ***bezpieczeństwa systemów informacyjnych*** *lub* ***ciągłości działania*** *... .*

Przedmiotu zamówienia nie należy traktować jako audyt w rozumieniu ustawy, a weryfikację stanu aktualnego (IsAs) i określenie stanu docelowego (ToBe) w zakresie wskazanym w SIWZ. Mając powyższe na uwadze, Zamawiający pozostawia zapisy SIWZ bez zmian, co uzasadnione jest również wielkością i różnorodnością podmiotów leczniczych będących operatorami usługi kluczowej.

Odpowiedź na pytanie nie stanowi zmiany treści SIWZ.

Dotychczasowy termin składania ofert, tj. w dniu 30 czerwca 2020 r. o godz. 11.00 nie ulega zmianie. Otwarcie ofert odbędzie się w dniu 30 czerwca 2020 r. o godz. 12.00.

Z poważaniem

ZASTĘPCA DYREKTORA

Marcin BOMBRYCH

Wyk. J.Gajewski - osobiście
T: 2612 B5

Nr sprawy: 15/ZP/20