Warszawa, 31 lipca 2018 r.

ODPOWIEDZI NA PYTANIA DO TREŚCI SIWZ

Dotyczy: postępowania o udzielenie zamówienia publicznego (Nr 30/18/PN) na świadczenie usług audytów bezpieczeństwa oraz testów penetracyjnych systemów i infrastruktury informatycznej Narodowego Centrum Badań i Rozwoju

Zamawiający, Narodowe Centrum Badań i Rozwoju, uprzejmie informuje, iż w dniu 30 lipca 2018r. do Zamawiającego wpłynęły drogą elektroniczną wnioski o wyjaśnienie treści specyfikacji istotnych warunków zamówienia (dalej SIWZ) i załączników do SIWZ zamieszczonych na stronie internetowej NCBR. Poniżej przedstawiam ich treść wraz z wyjaśnieniami udzielonymi przez Zamawiającego.

Pytanie 1

1. *Jak należy rozumieć warunek, o którym mowa w pkt 5.2.2. SIWZ:*
a. *czy Zamawiający żąda, aby jeden z konsultantów posiadał co najmniej jeden z wymienionych certyfikatów, o których mowa w punktach 5.2.2.3- 5.2.2.5 SIWZ i w punktach 5.2.2.6-5.2.2.7 SIWZ (czyli co najmniej dwa certyfikaty z których jeden z punktów 5.2.2.3-5.2.2.5 SIWZ, zaś drugi z punktów 5.2.2.6-5.2.2.7 SIWZ, ponieważ punkty 5.2.2.5 i 5.2.2.7 SIWZ zakończone są kropką, a pozostałe przecinkiem, co sugeruje, że te które zakończone są kropką kończą wymagania w danym zakresie)?*
b. *czy też wymagane jest posiadanie przez zespół 3 konsultantów wszystkich wymienionych certyfikatów, pomimo tego, że punkty 5.2.2.5 SIWZ oraz 5.2.2.7 SIWZ kończą się kropką, a punkty 5.2.2.3,5.2.2.4, 5.2.2.6 kończą się przecinkiem?*

Powyższe jest o tyle istotne, że w świetle treści SIWZ oraz udzielonych do SIWZ odpowiedzi na zadania w toku postępowania zapytania przez Wykonawców warunek, o którym mowa w punkcie 5.2.2 SIWZ stał się niezrozumiały.

Odpowiedź

Zamawiający informuje, że punkt 5.2.2.1 i 5.2.2.2 oznacza, że każdy z członków Zespołu musi spełniać kryterium, punkty 5.2.2.3, 5.2.2.4, 5.2.2.5, 5.2.2.6, 5.2.2.7 oznaczają, że przynajmniej jeden z członków Zespołu musi spełniać kryterium, czyli cały Zespół musi posiadać wszystkie wymienione certyfikaty, a czy jest to jeden członek posiadający wszystkich 5 certyfikatów, czy inny rozkład członek – posiadany certyfikat – tego Zamawiający nie określa.

Pytanie 2

Ad. odpowiedź na pyt. 9 do OPZ- dotyczące producenta bazy danych. Proszę o podanie producenta bazy danych, która ma być objęta testami, o których mowa w opisie przedmiotu zamówienia. Proszę o wskazanie wersji ww. bazy?
Wykonawca zwraca uwagę na treść art. 29 ust. 1 ustawy Pzp, który nakłada na Zamawiającego obowiązek opisania przedmiotu zamówienia w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględnienia wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty. Powyższe jest niewątpliwie okolicznością mającą wpływ na sporządzenie oferty wobec tego proszę o wskazanie ww. danych, analogicznie jak w udzielonej przez Zamawiającego odpowiedzi na pytanie numer 12 do OPZ.

Odpowiedź

Zamawiający używa baz danych: MS SQL, Sybase, MySQL – wersji oprogramowania baz danych nie podajemy na tym etapie postępowania.

Pytanie 3

Ad. odpowiedź na pyt. 14 do OPZ dotyczące zakresu prac. Co Zamawiający rozumie pod pojęciem „aktualizacja Zakresu Przedmiotu Zamówienia", o której mowa w § 1 ust. 3 wzoru umowy?
Wykonawca zwraca uwagę na to, że brak wyjaśnienia ww. pojęcia uniemożliwia dokonanie wyceny oferty w niniejszym zamówieniu, z uwagi na fakt, że zakres prac pozostaje nieznany.

Odpowiedź

Zamawiający, że w dniu 27.07.2018r. udzielił odpowiedzi na pytanie nr 14 w części nr II dotyczącej OPZ, tj. „Czy testy infrastruktury będzie można prowadzić zdalnie", Zamawiający udzielił wyczerpującej odpowiedzi: „Tak testy infrastruktury będzie można prowadzić zdalnie".

Pytanie 4

Zgodne z pkt 2 OPZ: „*Przedmiot Umowy obejmuje dwa tryby zamówień: audyt pełny i audyty ad hoc.*

a. *Raz w roku kalendarzowym Wykonawca zobowiązuje się do wykonania pełnego audytu aplikacji i infrastruktury, co oznacza usługi wymienione w pkt 1 a) i 1) b powyżej w zakresie całej infrastruktury i wszystkich systemów Zamawiającego określonych poniżej w tabeli Wykaz systemów Zamawiającego*
b. *Ilość zamówień na w trybie ad hoc audytów wybranych systemów lub aplikacji, lub ich części oraz bezpieczeństwa elementów infrastruktury, nie przekroczy w czasie trwania Umowy ilości 14 zamówień, przy czym rocznie będzie to maksymalnie 7*".

Powyższe wskazuje, że audyt pełny obejmuje zakres prac wskazany w pkt 1 a i 1 b, o których mowa w pkt 1 OPZ. W przypadku audytu ad hoc Zamawiający nie określił jego zakresu.
Wobec tego zwracam się z prośbą o wyjaśnienie treści OPZ poprzez wskazanie: jaki dokładnie zakres usług ma wykonać Wykonawca w ramach realizacji audytów ad hoc? oraz Zamawiający wskazał, że audyty ad hoc będą dotyczyły wybranych systemów lub aplikacji lub ich części oraz bezpieczeństwa elementów infrastruktury. Co Zamawiający rozumie pod pojęciem „wybranych"? (czyli jakich konkretnie? ewentualnie wybranych spośród czego?).

Odpowiedź

Pod pojęciem „wybranych" Zamawiający rozumie aplikacje lub elementy infrastruktury wybrane z załącznika nr 3 do Umowy. Intencją Zamawiającego przy audytach ad hoc jest zbadanie podatności jednej aplikacji (lub jej konkretnego modułu) lub infrastruktury (lub jej konkretnego elementu).

Pytanie 5

Czym się różni styk z siecią Internet, o którym mowa w pkt. 12 tabeli „Wykaz systemów Zamawiającego" od styku z siecią Internet, o którym mowa w pkt. 13 tabeli „Wykaz systemów Zamawiającego" w OPZ ?

Odpowiedź

W punkcie 12 tabeli „Wykaz systemów Zamawiającego" chodzi o systemy pocztowe na styku z Internetem.

W punkcie 13 tabeli „Wykaz systemów Zamawiającego" chodzi o cały styk (www. Cloud, wszystkie portale wystawione na zewnątrz).

Pytanie 6

Ile IP adresów ma obejmować test styku z siecią Internet opisany w pkt. 13 tabeli „Wykaz systemów Zamawiającego" w OPZ?

Odpowiedź

Zamawiający informuje, że odpowiedzi na pytanie udzielono przy pytaniu II 10 w piśmie z dnia 27.07.2018 r.

Pytanie 7

Ad. odpowiedź na pyt. 4 dot. zakresu testów penetracyjnych. Ile dokładnie jest aplikacji i elementów infrastruktury (IP, hostów)?

Odpowiedź

Zamawiający informuje, że odpowiedzi na pytanie udzielono przy pytaniu II 26, II 34 w piśmie z dnia 27.07.2018 r. oraz w tabeli „Wykaz systemów Zamawiającego" w OPZ.

Pytanie 8

Ad. odpowiedź na pyt. 5 dot. liczby komponentów aplikacji. Ile jest publicznie dostępnych komponentów każdej z aplikacji, które mają być objęte testami

Odpowiedź

Zgodnie z pozycjami tabeli „Wykaz systemów Zamawiającego" pkt 1 – wszystkie poza częścią dostępną dla pracowników NCBR, pkt 2 – wszystkie, poza częścią dostępną dla pracowników NCBR, pkt 3 – wszystkie, pkt 4 – wszystkie, pkt 5 – wszystkie, pkt 6 – wszystkie, pkt 7 – odpowiedzi udzielono przy pytaniu II 22 w piśmie z dnia 27.07.2018 r., pkt 8 - odpowiedzi udzielono przy pytaniu II 23 w piśmie z dnia 27.07.2018 r. r., pkt 9 - odpowiedzi udzielono przy pytaniu II 24 w piśmie z dnia 27.07.2018 r., pkt 10 – żadne, pkt 11 – wszystkie, pkt 12 – wszystkie.

Pytanie 9

Ad. odpowiedź na pyt. 20 dot. Portal ankiet. Ile jest ankiet?

Odpowiedź

Zamawiający informuje, że odpowiedzi na pytanie udzielono przy pytaniu II 20 w piśmie z dnia 27.07.2018 r., jeden formularz to jedna ankieta.

Pytanie 10

Ad. odpowiedź na pyt. 20 dot. analiza statyczna kodu. Zamawiający odpowiedział „Analiza statyczna kodu będzie wyłącznie potencjalnie zgłaszana w zleceniu ad hoc. Audyt roczny nie obejmuje audytu kodu.". Powyższe stoi w sprzeczności z zapisem OPZ pkt. 1. Ppkt. a. „Raz w roku kalendarzowym Wykonawca zobowiązuje się do wykonania pełnego audytu aplikacji i infrastruktury, co oznacza usługi wymienione w pkt 1 a) i 1) b powyżej w zakresie całej infrastruktury i wszystkich systemów Zamawiającego określonych poniżej w tabeli Wykaz systemów Zamawiającego". Prosimy o jednoznaczne określenie w SIWZ OPZ zakresu wymaganych prac (usług). W chwili obecnej rozbieżne treści, o których mowa powyżej uniemożliwiają dokonanie wyceny tego zamówienia.

Odpowiedź

Zamawiający dokonał poprawek OPZ w przedmiotowym zakresie, pkt 2 a OPZ otrzymuje brzmienie:

„ 1. Przedmiot Umowy obejmuje dwa tryby zamówień: audyt pełny i audyty ad hoc

a. Raz w roku kalendarzowym Wykonawca zobowiązuje się do wykonania pełnego audytu aplikacji i infrastruktury, co oznacza usługi wymienione w pkt 1 a) i 1) c powyżej w zakresie całej infrastruktury i wszystkich systemów Zamawiającego określonych poniżej w tabeli Wykaz systemów Zamawiającego"

Pytanie 11

Pkt. 1 OPZ brzmi: „w ramach Zamówienia, Wykonawca będzie zobowiązany do świadczenia usług polegających na wykonywaniu:

a) audytów bezpieczeństwa oraz testów penetracyjnych systemów IT,
b) audytów kodu źródłowego,
c) audytów bezpieczeństwa oraz testów penetracyjnych infrastruktury",

W pkt. 2 OPZ brak jest informacji o pkt. 1 c). Czego w takim razie dotyczy pkt. 1 c)? Czy pkt 1 c dotyczy audytów rocznych czy ad hoc? czy też dotyczy jeszcze innego zakresu prac?

Odpowiedź

Zamawiający informuje, że odpowiedzi udzielono przy pytaniu 10 powyżej, Zamawiający poprawił OPZ w tym zakresie.

Pytanie 12

Pkt. 3. OPZ w tabeli określa m.in. następujący zakres audytu kodu aplikacji: „Określenie zgodności ze standardami organizacji". Prosimy o przekazanie/opublikowanie standardów organizacji, o których mowa w tym punkcie.

Odpowiedź

Zamawiający wykreśla ten punkt, wiersz 1 z tabeli otrzymuje brzmienie:

1	Audyt kodu aplikacji webowej	• Określenie powierzchni ataku • Określenie obszarów podwyższonego ryzyka • Identyfikacja klas podatności • Weryfikacja wdrożonych zaleceń

Pytanie 13

W załączniku do SIWZ pt.: wykaz osób, Zamawiający w kolumnie imię i nazwisko w tym wykazie w pozycjach „data wykonania- usługa 1" trzykrotnie podał, że chodzi mu o datę wykonania tej samej usługi- tj. usługi 1, czy treść wykazu osób w powyższym zakresie jest prawidłowa?

Odpowiedź

Zamawiający informuje, że poprawił błędne odnośniki do usługi 1 w załączniku nr 6 do SIWZ.

Aktualny wzór wykazu osób załącznik nr 6 można pobrać ze strony internetowej BIP NCBR.

Pytanie 14

Czy zakres audytów ad hoc ma obejmować re-testy?

Odpowiedź

Tak, każdy audyt ad hoc to testy i re-testy, co wynika także ze wzoru zamówienia będącego załącznikiem nr 4 do Umowy

Pytanie 15

Tabela z Wykazem systemów Zamawiającego (OPZ) raport z testów (wiersz 16) oraz Retesty zakończone Raportem z retestów (wiersz 17), które nie są systemami. Prosimy o skorygowanie tabeli

Odpowiedź

Zamawiający skorygował tabelę „Wykaz systemów Zamawiającego" oraz zamieścił poprawiony opis przedmiotu zamówienia na stronie internetowej BIP NCBR.

Pytanie 16

Z uwagi na fakt, że powyższe zapytania bezsprzecznie wpływają na treść oferty, Wykonawca prosi o wydłużenie terminu składania i otwarcia ofert do dnia 24 sierpnia 2018 r. Niejednoznaczne lub też niespójne postanowienia powodują, że Wykonawcy muszą ponownie zapoznać się z całością opublikowanej na stronie Zamawiającego dokumentacji tego postępowania, celem dokonania wyceny prac, po uwzględnieniu odpowiedzi na zadane pytania. W związku z powyższym w pełni zasadnym jest przedłużenie terminu składania ofert do dnia, który umożliwi w rzeczywistości jej prawidłowe sporządzenie w oparciu o treść SIWZ oraz w oparciu o treść opublikowanych przez Zamawiającego odpowiedzi.

Odpowiedź

Zamawiający informuje, że w dniu 27.07.2018r. przedłużył termin składania ofert do dnia 03.08.2018 r.

Pytanie 17

W prowadzonym przez Państwa postępowaniu na „Świadczenie usług audytów bezpieczeństwa oraz testów penetracyjnych systemów i infrastruktury informatycznej Narodowego Centrum Badań i Rozwoju", w projekcie umowy (Załącznik 2) w par. 11 p-kt 1 jest zapis

• *W przypadku niewykonania Przedmiotu Umowy, Zamawiający może żądać od Wykonawcy zapłaty kary umownej w wysokości 25 % wynagrodzenia brutto, o którym mowa w § 6 ust. 1 Umowy.*
Co Państwo rozumiecie pod pojęciem "niewykonania Przedmiotu umowy"? Czy taka sytuacja dotyczy np. opóźnienia w przystąpieniu do realizacji testów i/lub opóźnienia w ich wykonaniu?

Odpowiedź

Przez niewykonanie Umowy Zamawiający rozumie sytuację, gdy Wykonawca w ogóle nie podejmie się świadczenia usług stanowiących Przedmiot Umowy. Pomimo skutecznie zawartej Umowy pomiędzy Stronami.
W § 11 ust. 2 Umowy, przewidujemy karę za nienależyte wykonanie Umowy. W ust. 3 Zamawiający wskazuje co uważa za nienależyte wykonanie Umowy tj. w szczególności wykonanie Przedmiotu Umowy z opóźnieniem tj. niezachowaniem terminów wynikających z Umowy oraz wykonanie Przedmiotu Umowy w sposób niezgodny z Umową lub ZPU, w tym realizację Umowy odbiegającą jakościowo od ustalonej przez Strony.

Zamawiający informuje, że w wyniku powyższych wyjaśnień nie jest konieczny dodatkowy czas na wprowadzenie zmian w ofertach, termin i miejsce składania ofert pozostają bez zmian.

Zatwierdzam

Piotr Zerhau – Dyrektor Działu Systemów Informatycznych