Warszawa, dnia 8 lutego 2017 roku

**Dotyczy: Wyjaśnień do treści zapytania ofertowego w ramach postępowania na „Przeprowadzenie audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji”.**

**Wyjaśnienia do zapytania ofertowego**

**Zamawiający – Centrum Projektów Polska Cyfrowa – informuje, że w przedmiotowym postępowaniu Wykonawcy zwrócili się do Zamawiającego z wnioskami o wyjaśnienie treści zapytania ofertowego. W związku z powyższym, Zamawiający udzielił poniższych odpowiedzi:**

**Pytanie nr 4:**

Jakie serwisy internetowe będą podlegały testom bezpieczeństwa?

Zamawiający z zapytaniu ofertowym napisał ogólnie, że zakres prac obejmuje „Sprawdzenie podatności serwisów internetowych” nie precyzując o jakie serwisy chodzi. Prosimy o wyspecyfikowanie serwisów, które mają być objęte sprawdzeniem podatności. Bez tej informacji nie jest możliwa wycena prac.

**Odpowiedź nr 4:**

Zamawiający posiada serwis internetowy pod adresem <http://cppc.gov.pl> , jeden serwis internetowy typu chmura do udostępniania i współdzielenia plików oraz trzy rodzaje aplikacji internetowych.

**Pytanie nr 7:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - prosimy o informację jaka jest ilość aplikacji/serwerów i w jakiej technologii zostały stworzone?

Zamawiający nie wyspecyfikował systemów użytkowych, które mają być objęte zakresem prac. Bez tej informacji nie jest możliwa wycena prac. Prosimy o wyspecyfikowanie systemów użytkowych, które mają być objęte zakresem prac.

**Odpowiedź nr 7:**

W udzielonej odpowiedzi nie wyspecyfikowano systemów użytkowych, ponieważ w rozumieniu Zamawiającego pytanie nie dotyczy wyspecyfikowania systemów użytkowych. Inwentaryzacja zasobów sieci lokalnej Zamawiającego, w tym serwerów i aplikacji z ich szczegółowym opisem, stanowi przedmiot zamówienia. Zamawiający oczekuje takich informacji od Wykonawcy po zakończeniu audytu.

**Pytanie nr 8:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - jakie funkcje realizują aplikacje/systemy podlegające testom?

Zamawiający nie wyspecyfikował niezbędnych informacji (np. liczba ekranów, lista funkcji, liczba ról, itp.) o systemach / aplikacjach, które mają być objęte zakresem prac. Bez tej informacji nie jest możliwa wycena prac. Prosimy o wyspecyfikowanie systemów użytkowych, które mają być objęte zakresem prac.

**Odpowiedź nr 8:**

**Inwentaryzacja zasobów sieci lokalnej Zamawiającego, w tym systemów i aplikacji z ich szczegółowym opisem, stanowi przedmiot zamówienia. Zamawiający oczekuje takich informacji od Wykonawcy po zakończeniu audytu.**

**Pytanie nr 9:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - jaka jest szacunkowa liczba stron/formularzy dla każdej z aplikacji/systemu?

Zamawiający nie wyspecyfikował niezbędnych informacji (np. liczba ekranów, lista funkcji, liczba ról, itp.) o systemach / aplikacjach, które mają być objęte zakresem prac. Bez tej informacji nie jest możliwa wycena prac. Prosimy o wyspecyfikowanie systemów użytkowych, które mają być objęte zakresem prac.

**Odpowiedź nr 9:**

Inwentaryzacja zasobów sieci lokalnej Zamawiającego, w tym systemów i aplikacji z ich szczegółowym opisem, stanowi przedmiot zamówienia. Zamawiający oczekuje takich informacji od Wykonawcy po zakończeniu audytu.

**Pytanie nr 10:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - czy aplikacje/systemy posiadają mechanizm logowania? Jeśli tak, prosimy podanie ile różnych profili użytkownika obsługuje i czy wszystkie będą podlegały testom?

**Odpowiedź nr 10:**

W pytaniu nie sprecyzowano jakich dokładnie profili i logowania dotyczy pytanie. Czy chodzi o profile pojedynczych użytkowników w każdej aplikacji / systemie, czy może profile grup użytkowników takich jak Administratorzy, użytkownicy, itp. Tak samo w przypadku logowania, czy pytanie dotyczy zapisywania zdarzeń systemowych w plikach log czy dotyczy rejestracji użytkowników w systemie. W związku z nieprecyzyjnie sformułowanym pytaniem, Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.

**Pytanie nr 12:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - prosimy o informację z jakich protokołów komunikacyjnych korzystają określone aplikacje oraz jakie API udostępniają?

Prosimy o wyspecyfikowanie nazw systemów, wersji oraz nazw producentów, w celu ustalenia jakie API one udostępniają.

**Odpowiedź nr 12:**

Inwentaryzacja systemów Zamawiającego z ich szczegółowym opisem stanowi przedmiot zamówienia. Zamawiający oczekuje takiej informacji od Wykonawcy po zakończeniu audytu.

**Pytanie nr 16:**

Czy Wykonawca może realizować badanie zgodności poszczególnych procesów na próbie, czy ma zostać poddana badaniu cała **populacja**? Prosimy o doprecyzowanie w każdym z elementów badania?

Zgodnie ze profesjonalnymi standardami prowadzenia audytów, audyt prowadzi się na próbce, a nie całej populacji.

**Odpowiedź nr 16:**

Badaniu zgodności poszczególnych procesów ma zostać poddana cała populacja.

**Pytanie nr 20:**

Prosimy o przesłanie treści klauzuli poufności, którą należy podpisać przed rozpoczęciem audytu.

W opublikowanym na stronie www Zamawiającego zapytaniu ofertowym brak jest załącznika nr 5.

**Odpowiedź nr 20:**

Treść przedmiotowej klauzuli znajduje się w załączniku nr 5 do opublikowanej, zaktualizowanej wersji zapytania ofertowego dostępnego pod linkiem <https://cppc.gov.pl/bip/zamowienie-o-wartosci-ponizej-kwoty-30-000-euro-na-przeprowadzenie-audytu-informatycznego-z-zakresu-inwentaryzacji-zasobow-sprzetowych-i-programowych-systemu-informatycznego-oraz-audyt-bezpie/>

**Pytanie nr 9:**

Odnośnie pkt. III. 1 Szczegółowy zakres przetwarzania i ochrony danych osobowych:

**a.** Prosimy o wyspecyfikowanie aktów prawnych, o których mowa w pkt. 1.

OP: prosimy o wskazanie adresu URL, pod którym znajduje się treść zmienionego punktu.

**Odpowiedź dotycząca lit. a.:**

Zamawiający dokonał zmiany treści pkt. 1 w rozdziale III. Zmieniona oraz aktualna treść opisu przedmiotu zamówienia w tym zakresie została opublikowana na portalu Baza Konkurencyjności pod linkiem <https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/publication/view/1017337> oraz na stronie internetowej Zamawiającego pod linkiem <https://cppc.gov.pl/bip/zamowienie-o-wartosci-ponizej-kwoty-30-000-euro-na-przeprowadzenie-audytu-informatycznego-z-zakresu-inwentaryzacji-zasobow-sprzetowych-i-programowych-systemu-informatycznego-oraz-audyt-bezpie/>

**c.** Prosimy o informację ile jest zbiorów danych osobowych.

OP: prosimy o wskazanie adresu URL, pod którym znajduje się treść zmienionego punktu.

**Odpowiedź dotycząca lit. c.:**

Zamawiający dokonał zmiany treści pkt. 1 w rozdziale III. Zmieniona oraz aktualna treść opisu przedmiotu zamówienia w tym zakresie została opublikowana na portalu Baza Konkurencyjności pod linkiem <https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/publication/view/1017337> oraz na stronie internetowej Zamawiającego pod linkiem <https://cppc.gov.pl/bip/zamowienie-o-wartosci-ponizej-kwoty-30-000-euro-na-przeprowadzenie-audytu-informatycznego-z-zakresu-inwentaryzacji-zasobow-sprzetowych-i-programowych-systemu-informatycznego-oraz-audyt-bezpie/>

**Pytanie nr 22:**

Odnośnie pkt. III. 2. Szczegółowy zakres bezpieczeństwa systemów informatycznych:

**e.** Ile jest serwisów internetowych, które mają być objęte audytem?

Zamawiający z zapytaniu ofertowym napisał ogólnie, że zakres prac obejmuje „Sprawdzenie podatności serwisów internetowych” nie precyzując o jakie serwisy chodzi. Prosimy o wyspecyfikowanie serwisów, które mają być objęte sprawdzeniem podatności. Bez tej informacji nie jest możliwa wycena prac.

**Odpowiedź dotycząca lit. e.:**

Audytem ma być objęte do sześciu serwisów. Między innymi serwis internetowy pod adresem <http://cppc.gov.pl> , serwis internetowy typu chmura do udostępniania i współdzielenia plików oraz trzy rodzaje aplikacji internetowych.

**f.** Prosimy o przesłanie linków do serwisów internetowych, które mają być objęte audytem.

Bez linków do serwisów lub informacji o tych serwisach (liczba stron / podstron, liczba formularzy, liczba ról, itp.) nie jest możliwa wycena testów. Prosimy o wyspecyfikowanie informacji, które umożliwią wycenę.

**Odpowiedź dotycząca lit. f.:**

Zamawiający posiada serwis internetowy pod adresem <http://cppc.gov.pl> , jeden serwis internetowy typu chmura do udostępniania i współdzielenia plików oraz trzy rodzaje aplikacji internetowych. Każda z nich posiada do 10 podstron i do 2 formularzy oraz do 2 ról.

**Pytanie nr 63:**

Czy inwentaryzacja aktywów ma zakładać tryb manualny (weryfikacja fizyczna aktywa, oznacza w praktyce, że audytor uda się do pokoju / biura w którym znajduje się aktywo)

W związku z dodatkowymi pytaniami prosimy o wydłużenie terminu składania ofert do 10 lutego 2017 r.

**Odpowiedź nr 63:**

Zamawiający wydłużył termin składania ofert do dnia 10 lutego 2017 roku do godz. 10:00.

**Pytanie:**

W sprostowaniu do wyjaśnień oraz zaktualizowanym zapytaniu ofertowym Zamawiający w Rozdziale V. Warunki udziału w postępowaniu, punkt 2. Dysponowanie osobami zdolnymi do wykonania zamówienia wymaga posiadania co najmniej dwóch osób w roli Ekspert ds. audytu IT i bezpieczeństwa, posiadających m.in. następujące kwalifikacje i doświadczenie zawodowe:

• wykształcenie wyższe;

• posiada co najmniej 3-letnie doświadczenie w zakresie przeprowadzania audytów odpowiadających swoim zakresem przedmiotowi niniejszego zamówienia;

• co najmniej jeden z ekspertów powinien posiadać aktualne certyfikaty Audytora Wiodącego norm: ISO 27001 i ISO 22301 lub równoważne;

• pozostali członkowie zespołu eksperckiego powinni posiadać certyfikat Audytora Wiodącego norm: ISO 27001 lub ISO 22301 lub równoważne;

• co najmniej jeden z ekspertów powinien posiadać aktualny certyfikat z zakresu zarządzania projektami PRINCE 2 lub równoważny (…).

Uprzejmie proszę o potwierdzenie, iż wymaganie dotyczące posiadania certyfikatu PRINCE 2 lub równoważnego dotyczy jednego z członków zespołu eksperckiego (któregokolwiek), a nie ekspertów występujących w roli audytorów. Takie wymaganie adresowane do audytorów byłoby niezgodne i nadmiarowe w odniesieniu do roli pełnionej przez nich w przedmiotowym postępowaniu.

**Odpowiedź:**

Wymaganie dotyczące posiadania certyfikatu PRINCE 2 lub równoważnego dotyczy jednego, któregokolwiek członka zespołu eksperckiego. Nie jest to wymaganie niezbędne sformułowane w odniesieniu do ekspertów występujących w roli audytorów.

**Pytanie:**

W Rozdziale III OPZ punkt 2. „Szczegółowy zakres bezpieczeństwa systemów informatycznych”, w tym wymieniony punkt 4. Sprawdzenie podatności serwisów internetowych. Do tego punktu odnoszą się m.in. pytania nr 4, 8, 9 i 10. Uprzejmie prosimy o ponowne udzielenie odpowiedzi na ww. pytania mając na uwadze, iż pytający odnosi się do serwisów internetowych posiadanych przez Zamawiającego, a wspomnianych przez niego w punkcie 4. Na pytania nr 4, 9 - Zamawiający nie udzielił odpowiedzi w tym zakresie, zaś na pytania 8, 9, 10 – Zamawiający udzielił odpowiedzi cząstkowej, która w niewielkim tylko stopniu przyczynia się do lepszego zrozumienia zakresu zamówienia.

**Odpowiedź:**

Zamawiający posiada serwis internetowy pod adresem http://cppc.gov.pl , jeden serwis internetowy typu chmura do udostępniania i współdzielenia plików oraz trzy rodzaje aplikacji internetowych.

Ponadto Zamawiający przypomina, iż inwentaryzacja zasobów sieci lokalnej Zamawiającego, w tym systemów i aplikacji z ich szczegółowym opisem, stanowi przedmiot zamówienia. Zamawiający oczekuje takich informacji od Wykonawcy po zakończeniu Audytu.

Wykonawcy nie sprecyzowali w swoich wnioskach, jakich dokładnie profili i logowania dotyczy pytanie. Czy chodzi o profile pojedynczych użytkowników w każdej aplikacji / systemie czy może profile grup użytkowników takich jak Administratorzy, użytkownicy, itp. Tak samo w przypadku logowania, czy pytanie dotyczy zapisywania zdarzeń systemowych w plikach log czy dotyczy rejestracji użytkowników w systemie. W związku z nieprecyzyjnie sformułowanym pytaniem, Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.