

Zapytanie Ofertowe Nr 2023-7175-142933**Zaprojektowanie systemu zarządzania cyberbezpieczeństwem**

1. W ramach projektu pt. „Solaris CyberSecure Connectivity” dofinansowanego w ramach Poddziałania 1.1.1 Programu Operacyjnego Inteligentny Rozwój 2014-2022 współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego

Nr Wniosku: POIR.01.01.01-00-0298/22

Zamawiający:

Nazwa Zamawiającego	Solaris Bus & Coach S.A.
Adres siedziby	ul. Obornicka 46, Bolechowo-Osiedle, 62-005 Owińska, Polska
NIP	PL5240015630
Numer KRS	0000236619
REGON	010498995
Kapitał zakładowy	160.169.580,00 PLN, w całości wpłacony
Osoba do kontaktu	Justyna Sikorska
Nr telefonu	T: +48 697 949 771
Adres e-mail	zapytanie.projekt@solarisbus.com

2. Tryb udzielania zamówienia:

Postępowanie o udzielenie zamówienia prowadzone jest w trybie konkurencyjnym z zachowaniem zasady uczciwej konkurencji, równego traktowania, jawności i przejrzystości w oparciu o procedurę opisaną w „Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020”. Do niniejszego zapytania ofertowego nie mają zastosowania przepisy Ustawy z dnia 29 stycznia 2004r. Prawo Zamówień Publicznych poza przypadkami wyraźnie zastrzeżonymi w wyżej przywołanych wytycznych.

3. Miejsce, termin i sposób składania ofert:

- a. Termin składania ofert: 20.02.2023
- b. Ofertę należy przesłać w oryginale, podpisanym przez osobę/osoby umocowaną/umocowane do reprezentacji danego wykonawcy zgodnie z informacją zawartą w rejestrze lub podpisaną przez osobę umocowaną na mocy udzielonego pełnomocnictwa, na adres Zamawiającego ul. Obornicka 46, Bolechowo-Osiedle, 62-005 Owińska (koperta opatrzona dopiskiem Justyna Sikorska oraz numerem zapytania ofertowego 2023-7175-142933)

Alternatywnie ofertę można przesłać za pośrednictwem poczty elektronicznej w formie skanu podpisanego przez osobę/osoby umocowaną/umocowane do reprezentacji danego oferenta zgodnie z informacją zawartą w rejestrze lub podpisaną przez osobę umocowaną na mocy udzielonego pełnomocnictwa. Oferty w formie skanu należy przysyłać na adres: zapytanie.projekt@solarisbus.com. W razie złożenia oferty za pośrednictwem poczty email, na

żądanie Zamawiającego, wykonawca zobowiązany jest do niezwłocznego dostania oryginału złożonej oferty pod rygorem jej odrzucenia.

Za moment wpływu oferty uważa się chwilę dostarczenia do Zamawiającego oferty za pośrednictwem poczty elektronicznej lub dostarczenia oryginału oferty drogą pocztową – w zależności od wyboru metody dostarczenia oferty przez Wykonawcę.

Wykonawca ponosi wyłączną odpowiedzialność i ryzyko za dostarczenie oferty – nieotrzymanie oferty przez Zamawiającego lub otrzymanie jej po terminie składania ofert, bez względu na przyczynę, nie może być powodem roszczeń danego wykonawcy wobec Zamawiającego. Wykonawca ma prawo żądać wydania zaświadczenia o otrzymaniu oferty przez Zamawiającego – wraz z podaniem ilości otrzymanych przez Zamawiającego stron.

Każda ze stron oferty musi być parafowana przez danego wykonawcę.

- c. Oferty złożone po terminie nie będą rozpatrywane. Decyduje data i czas wpłynięcia oferty do Zamawiającego.
- d. Wykonawca może przed upływem terminu składania ofert zmienić lub wycofać swoją ofertę.
- e. W toku porównywania i oceny ofert Zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych ofert. Odmowa udzielenia odpowiedzi na zadane pytanie lub brak odpowiedzi w określonym terminie może stanowić podstawę do odrzucenia oferty.
- f. W toku porównywania i oceny ofert Zamawiający może żądać od wykonawców uzupełnienia złożonych ofert. Brak uzupełnienia oferty w określonym terminie może stanowić podstawę do odrzucenia oferty.
- g. Zapytanie ofertowe zamieszczono na stronie: www.bazakonkurencyjnosci.gov.pl
- h. Wszelkie koszty związane z przygotowaniem oferty ponosi wykonawca.
- i. Do oferty należy dołączyć dokument, z którego wynika umocowanie osoby/osób podpisującej/podpisujących ofertę do reprezentowania wykonawcy (odpis z Krajowego Rejestru Sądowego lub pełnomocnictwo).

4. Opis przedmiotu zamówienia:

Przedmiotem zamówienia jest usługa badawcza polegająca na:

- Szczegółowej analizie dokumentacji technicznej i procesowej związanej z autobusami produkowanymi przez firmę Solaris pod kątem Cyberbezpieczeństwa (rozumianego jako co najmniej spełnienie regulaminów 155 i 156 EKG ONZ).
- Opracowanie wytycznych i zakresu niezbędnych zmian dla dokumentacji technicznej i opracowanie całości dokumentacji procesowej uwzględniającej niezbędne zmiany, związanej z autobusami produkowanymi przez firmę Solaris, aby spełnić wymagania Cyberbezpieczeństwa
- Opracowanie metodologii i przeprowadzenie testów penetracyjnych weryfikujących skuteczność ochrony pojazdów przed cyberatakami dla krytycznych systemów autobusów. (maksymalnie kilkanaście w tym, m.in układ napędowy, hamulcowy, kierowniczy).
- Testy będą stacjonarne / stanowiskowe oraz w warunkach zbliżonych do warunków eksploatacyjnych na autobusie testowym.

Opracowana dokumentacja i rozwiązania muszą zapewnić zgodność z obowiązującymi dla autobusów regulacjami prawnymi na rynku europejskim.

Opracowana dokumentacja i rozwiązania muszą być zgodne i umożliwić uzyskanie certyfikatów zarządzania cyberbezpieczeństwem i aktualizacjami oprogramowania na pojazdach, oraz uzyskanie / rozszerzenie homologacji „typu”.

a. Cel zamówienia:

Zaprojektowanie systemu zarządzania cyberbezpieczeństwem w ramach projektu nr POIR.01.01.01-00-0298/22 z przekazaniem praw własności intelektualnej dla przedmiotu postępowania.

b. Przedmiot zamówienia:

Przedmiotem zamówienia jest usługa badawcza polegająca na:

- Szczegółowej analizie dokumentacji technicznej i procesowej związanej z autobusami produkowanymi przez firmę Solaris pod kątem Cyberbezpieczeństwa (rozumianego jako co najmniej spełnienie regulaminów 155 i 156 EKG ONZ).

- Opracowanie wytycznych i zakresu niezbędnych zmian dla dokumentacji technicznej i opracowanie całości dokumentacji procesowej uwzględniającej niezbędne zmiany, związanej z autobusami produkowanymi przez firmę Solaris, aby spełnić wymagania Cyberbezpieczeństwa

- Opracowanie metodologii i przeprowadzenie testów penetracyjnych weryfikujących skuteczność ochrony pojazdów przed cyberatakami dla krytycznych systemów autobusów. (maksymalnie kilkanaście w tym, m.in układ napędowy, hamulcowy, kierowniczy). Testy będą stacjonarne / stanowiskowe oraz w warunkach zbliżonych do warunków eksploatacyjnych na autobusie testowym.

Opracowana dokumentacja i rozwiązania muszą zapewnić zgodność z obowiązującymi dla autobusów regulacjami prawnymi na rynku europejskim.

Opracowana dokumentacja i rozwiązania muszą być zgodne i umożliwić uzyskanie certyfikatów zarządzania cyberbezpieczeństwem i aktualizacjami oprogramowania na pojazdach, oraz uzyskanie / rozszerzenie homologacji „typu”.

Etap 1. Badania i analizy

Pierwszy etap będzie polegał na wykonaniu badań i analiz procesów i produktów firmy Solaris.

Pierwszy etap będzie polegał na szczegółowej analizie dokumentacji technicznej i procesowej związanej z autobusami produkowanymi przez firmę Solaris pod kątem Cyberbezpieczeństwa (rozumianego jako co najmniej spełnienie regulaminów 155 i 156 EKG ONZ).

Analiza będzie dotyczyć całego aktualnego portfolio produktowego firmy Solaris pod kątem przygotowania zasad zarządzania cyberbezpieczeństwem pojazdów na etapie rozwoju, produkcji i poprodukcyjnym.

W ramach zadania należy wykonać co najmniej niżej wymienione badania, analizy oraz opracować rekomendacje dotyczące:

- Zdefiniowania ITEMów

Przez itemy rozumiemy układy funkcjonalne, używane w pojazdach produkowanych przez firmę Solaris, które realizują określoną funkcję, np. zmiana kierunku ruchu i mogą zostać zmanipulowane.

Założeniem jest, że Itemami takimi będą m.in. układ kierowniczy ze wszystkimi jego odmianami jako jeden item.

- Zdefiniowanie Aktywów

Poprzez Aktywa rozumiemy grupy komponentów używanych w pojazdach produkowanych przez firmę Solaris, które wysyłają, przesyłają lub przetwarzają dane, które mogą zostać zmanipulowane.

Komponentami takimi będą m.in. sterownik silnika spalinowego ze wszystkimi jego odmianami jako jedno aktywo.

Szacuje się, że aktywów, zdefiniowanych jak wyżej, będzie co najmniej 20, a nie więcej niż 40.

- Analizy ryzyka

W ramach pracy należy przeprowadzić analizy TARA (zgodnie z normą ISO 21434) wraz z rekomendacją akceptowalnych poziomów CAL. Analizy TARA powinny obejmować całe portfolio produktowe pod kątem zdefiniowanych wcześniej itemów i aktywów ważnych z punktów widzenia cyberbezpieczeństwa oraz bezpieczeństwa funkcjonalnego.

- Analiza Procesów

Należy dokonać szczegółowej analizy procesów związanych z cyberbezpieczeństwem (w rozumieniu Regulaminu EKG ONZ 155 i 156). Wraz z rekomendacjami co najmniej w zakresie zmian dot. procesów analizy ryzyka, zarządzania podatnościami, zarządzania bezpieczeństwem dostawców, zarządzania w organizacji, zarządzania aktualizacjami oprogramowania, raportowania informacji o cyberatakach i podatnościach.

- Analiza interfejsów pojazdów i ich zabezpieczeń

Należy zbadać i określić możliwe interfejsy zewnętrzne pojazdu oraz istniejące sposoby zabezpieczeń.

- Analiza możliwych wektorów ataku na pojazdy produkowane przez firmę Solaris

Należy zbadać i określić w jaki sposób można przeprowadzić ataki hakerskie na pojazdy Solaris.

- Identyfikacja i analiza krytycznych systemów bezpieczeństwa (napęd, układ kierowniczy, funkcje bezpieczeństwa)

Należy zdefiniować i przeprowadzić analizę jaki wpływ na bezpieczeństwo pojazdu mogą mieć skuteczne ataki hakerskie zmieniające parametry działania systemów krytycznych.

- Analiza zarządzania aktualizacjami

Analiza procesów pod kątem sposobu zarządzania aktualizacjami oprogramowania związanego z funkcjonowaniem produkowanych przez Zlecającego autobusów na wszystkich etapach życia tych produktów.

Przygotowanie wniosków i rekomendacji w zakresie opracowania bezpiecznego systemu zarządzania aktualizacjami oprogramowania spełniającego wymagania zawarte w regulaminie R156 EKG ONZ oraz praktyki i specyfikę branży autobusów na rynku europejskim.

Data rozpoczęcia etapu 1: 01.03.2023

Data zakończenia etapu 1: 30.05.2023

Etap 2. Opracowanie dokumentacji dot. Sytemu Zarządzania Cyberbezpieczeństwem

Drugi etap polegać będzie na opracowaniu dokumentacji procesowej oraz dokumentacji zawierającej wytyczne z zakresu cyberbezpieczeństwa obejmujące wszystkie typy pojazdów produkowanych przez firmę Solaris. Dokumentacja musi być zgodna z wymaganiami regulaminów EKG ONZ 155 i 156.

Dokumentację należy opracować w następujących zakresach:

- Dokumentacja procesowa => propozycje i wytyczne dot. niezbędnych zmian w procesach firmowych w tym dot. dostawców i klientów
- Dokumentacja konstrukcyjna => propozycje i wytyczne dot. niezbędnych zmian w dokumentacji konstrukcyjnej elementów składowych produkowanych pojazdów
- Dokumentacja związana z systemem zarządzania cyberbezpieczeństwem (Work Products) => dokumentacja niezbędna do spełnienia wymogów związanych z cyberbezpieczeństwem.

Dokumentacja (Work Product) wymagana w systemie zarządzania cyberbezpieczeństwem, którą należy opracować musi dotyczyć minimum Aktywów i Itemów zdefiniowanych w Etapie 1.

Dokumentacja (Work Product) wymagana w systemie zarządzania cyberbezpieczeństwem, którą należy opracować musi ponadto zawierać minimum:

- przeprowadzone analizy TARA obejmujące wszystkie produkowane przez firmę Solaris typy pojazdów oraz analizy TARA szczegółowe dla wszystkich wcześniej wymienionych aktywów i itemów,
- metodykę wyznaczania poziomu CAL dla systemów krytycznych oraz akceptowanego poziom CAL w firmie Solaris,
- procedury związane z cyklem życia pojazdu,
- najbardziej prawdopodobne scenariusze wektorów ataku na pojazdy Solaris,
- oceny kategoryzacji i łagodzenia zidentyfikowanych ryzyk,
- obowiązujące w firmie Solaris standardy kryptograficzne,
- opis procesu gwarantującego, że ryzyka są zidentyfikowane i właściwie zarządzane,
- opis procesu gwarantującego, że analiza ryzyka jest ciągle aktualna,
- opis procesu dostarczania danych, aby wesprzeć analizę udanych i nieudanych cyberataków,

- opis procesu dotyczącego identyfikacji oprogramowania na sterownikach wszystkich pojazdów wyprodukowanych przez firmę Solaris (RxSWIN) w całym cyklu życia,
- opis procesów dotyczących systemu zarządzania aktualizacjami sterowników we wszystkich produkowanych przez firmę Solaris pojazdach w całym cyklu życia.

Integralną częścią zlecenia jest instruktaż w zakresie efektów prac zrealizowanych w ramach etapu.

Ponadto należy opracować ogólną koncepcję cyberbezpieczeństwa pojazdów produkowanych przez firmę Solaris.

Data rozpoczęcia etapu 2: 01.03.2023

Data zakończenia etapu 2: 30.06.2023

Etap 3. Walidacja cyberbezpieczeństwa OnePlatform i przeprowadzenie badań laboratoryjnych

Etap 3 będzie polegał na opracowaniu dokumentacji zawierającej procedury przeprowadzenia badań laboratoryjnych z zakresu cyberbezpieczeństwa oraz walidacji modułu „OnePlatform”.

Moduł OnePlatform odpowiada za Connecivity pojazdu, czyli jest systemem wymiany danych autobusu (zarówno na jego pokładzie jak i ze środowiskiem zewnętrznym).

W ramach etapu należy:

- Opracować i opisać scenariusze badań krytycznych systemów bezpieczeństwa (napęd, układ kierowniczy, funkcje bezpieczeństwa). Należy zbadać i przetestować na stanowisku testowym jaki wpływ na bezpieczeństwo pojazdu może mieć skuteczny atak hakerski zmieniający parametry działania systemów krytycznych.
- Opracować dokumentację zawierającą procedurę testów penetracyjnych oraz przeprowadzić testy penetracyjne co najmniej dla krytycznych systemów pojazdów w warunkach laboratoryjnych (Testy będą przeprowadzone, aż do osiągnięcia poziomu 90% odporności systemu. W przypadku nieosiągnięcia tego parametru konieczne będzie dokonanie usprawnień systemu i powtórzenie testów).
- Opracować dokumentację zawierającą procedurę testów penetracyjnych oraz przeprowadzić testy penetracyjne dla interfejsów komunikacyjnych (autobusu i OnePlatform) w warunkach laboratoryjnych. (Testy będą przeprowadzone aż do osiągnięcia poziomu 90% odporności systemu. W przypadku nieosiągnięcia tego parametru konieczne będzie dokonanie usprawnień systemu i powtórzenie testów).
- Opracować dokumentację zawierającą wytyczne dla cyberbezpieczeństwa dla OnePlatform.
- Opracować dokumentację opisującą walidację pod kątem cyberbezpieczeństwa OnePlatform.
- Opracować dokumentację zawierającą wytyczne do co najmniej 1 systemu detekcji nieuprawnionego dostępu do pojazdu (sieć CAN-BUS) przez interfejsy zewnętrzne.
- Opracować dokumentację dla pozostałych wymagań systemu zarządzania cyberbezpieczeństwem i aktualizacjami oprogramowania, które wynikają z wymagań R155 i R156, zawierające m.in:
 - a) pełne przygotowanie kompletu dokumentacji procesów do uzyskania certyfikatu zgodności z Systemem Zarządzania Cyberbezpieczeństwem,

b) pełne przygotowanie kompletu dokumentacji procesów do uzyskania certyfikatu zgodności z Systemem Zarządzania Aktualizacjami Oprogramowania,

c) przygotowanie kompletu dokumentacji procesów dla celów homologacyjnych dla wszystkich produkowanych typów pojazdów.

Integralną częścią zlecenia jest instruktaż w zakresie efektów prac zrealizowanych w ramach etapu.

Data rozpoczęcia etapu 3: 01.05.2023

Data zakończenia etapu 3: 30.10.2023

Etap 4. Testy penetracyjne w warunkach zbliżonych do rzeczywistych

Etap czwarty będzie polegać na przeprowadzeniu testów penetracyjnych na przygotowanym autobusie testowym w warunkach zbliżonych do operacyjnych (co najmniej 5km – np. tor wokół zakładu produkcyjnego w Bolechowie)

W ramach etapu należy:

- Opracować dokumentację opisującą scenariusze do testów penetracyjnych dla krytycznych systemów pojazdów, interfejsów komunikacyjnych, w tym OnePlatform, w warunkach zbliżonych do rzeczywistych.

- Przeprowadzić testy penetracyjne dla krytycznych systemów pojazdów, interfejsów komunikacyjnych w tym One Platform, w warunkach zbliżonych do rzeczywistych. (Testy będą przeprowadzone, aż do osiągnięcia poziomu 90% odporności systemu. W przypadku nieosiągnięcia tego parametru konieczne będzie dokonanie usprawnień systemu i powtórzenie testów. Testy będą wykonane przede wszystkim na przeznaczonym do tego zadania pojeździe). Rzeczywiste sytuacje operacyjne to m.in. jazda, zmiana pasa ruchu, przystanek autobusowy, ładowanie, tankowanie. Krytyczne systemy bezpieczeństwa pojazdów to m.in: układ napędowy, hamulcowy, kierowniczy.

- Opracować raport z przeprowadzonych testów.

Integralną częścią zlecenia jest instruktaż w zakresie efektów prac zrealizowanych w ramach etapu.

Data rozpoczęcia etapu 4: 01.10.2023

Data zakończenia etapu 4: 15.12.2023

Etap 5. Testy penetracyjne w warunkach drogowych

Etap piąty będzie polegać na przeprowadzeniu testów penetracyjnych na przygotowanym autobusie testowym w warunkach rzeczywistych (co najmniej 100 km np. lotnisko) w celu potwierdzenia osiągnięcia odporności na penetrację systemu cyberbezpieczeństwa na określonym poziomie. Testy rzeczywiste powinny uwzględniać innych aktorów takich jak osoby postronne, samochody oraz długi czas ekspozycji na ryzyko, np. postój na zajezdni.

W ramach etapu należy:

- Opracować i opisać scenariusze testów penetracyjnych dla krytycznych systemów pojazdów, interfejsów komunikacyjnych w tym OnePlatform, w warunkach drogowych.
- Przeprowadzić testy penetracyjne dla krytycznych systemów pojazdów, interfejsów komunikacyjnych w tym One Platform, w warunkach zbliżonych do rzeczywistych. W przypadku nieosiągnięcia tego parametru konieczne będzie dokonanie usprawnień systemu i powtórzenie testów. Testy będą wykonane przede wszystkim na przeznaczonym do tego zadania pojeździe). Rzeczywiste sytuacje operacyjne to m.in. jazda, zmiana pasa ruchu, przystanek autobusowy, ładowanie, tankowanie. Krytyczne systemy bezpieczeństwa pojazdów to m.in: układ napędowy, hamulcowy, kierowniczy.
- Opracować raport z przeprowadzonych testów
- Przeprowadzić próbny audyt powyższych systemów zarządzania cyberbezpieczeństwem, systemu zarządzania aktualizacjami software i kompletności dokumentacji potrzebnej do przeprowadzenia homologacji „typu” dla wszystkich typów pojazdów produkowanych przez firmę Solaris w aspekcie elektrycznej i elektronicznej architektury i zewnętrznych interfejsów komunikacyjnych.

Data rozpoczęcia etapu 5: 01.10.2023

Data zakończenia etapu 5: 15.12.2023

Oferta powinna uwzględniać następujące etapy:

Etap 1: Badania i analizy (01.03-30.05.2023)

Etap 2: Opracowanie dokumentacji dot. Sytemu Zarządzania Cyberbezpieczeństwem (01.03-30.06.2023)

Etap 3: Walidacja cyberbezpieczeństwa OnePlatform i przeprowadzenie badań laboratoryjnych (01.05-30.10.2023)

Etap 4: Testy penetracyjne w warunkach zbliżonych do rzeczywistych (01.10-15.12.2023)

Etap 5: Testy penetracyjne w warunkach drogowych (01.10-15.12.2023)

Równoważność

Wszędzie tam, gdzie przedmiot zamówienia jest opisany poprzez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu dopuszcza się zastosowanie rozwiązań równoważnych w stosunku do opisanych, pod warunkiem, że będą one posiadały co najmniej takie same lub lepsze parametry techniczne i funkcjonalne i nie obniżą określonych w dokumentacji standardów.

Wszędzie tam, gdzie przedmiot zamówienia opisany jest przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych dopuszcza się rozwiązania równoważne opisywanym.

c. Kody CPV zamówienia:

73300000-5 – projekt i realizacja badań oraz rozwój

79417000-0 – Usługi doradcze w zakresie bezpieczeństwa

34121000-1 - Autobusy i autokary

d. Końcowy termin realizacji zamówienia: 15.12.2023

e. Termin związania ofertą (termin ważności oferty): 30 dni kalendarzowych licząc od dnia następującego po dniu, w którym przypada termin składania ofert. Na żądanie Zamawiającego oferenci mogą być jednokrotnie zobowiązani do przedłużenia terminu związania ofertą o dodatkowe 60 dni, pod rygorem odrzucenia oferty.

f. Zamawiający nie dopuszcza możliwość składania ofert częściowych.

g. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

5. Warunki udziału w postępowaniu:

a. Wykluczeniu z postępowania podlegają Wykonawcy, którzy są powiązani osobowo lub kapitałowo z Zamawiającym.

Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzaniem procedury wyboru wykonawcy, a wykonawcą, polegające w szczególności na:

- uczestniczeniu w spółce, jako wspólnik spółki cywilnej lub spółki osobowej;
- posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez instytucję zarządzającą projektem;
- pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
- pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.

Osoby wykonujące czynności w postępowaniu o udzielenie zamówienia podlegają wyłączeniu, jeżeli ubiegają się o udzielenie tego zamówienia lub zostały prawomocnie skazane za przestępstwo popełnione w związku z postępowaniem o udzielenie zamówienia, przestępstwo przekupstwa, przestępstwo przeciwko obrotowi gospodarczemu lub inne przestępstwo popełnione w celu osiągnięcia korzyści majątkowych.

b. Warunki

Wiedza i doświadczenie

Wykonawca posiada wiedzę i doświadczenie, tj. w okresie ostatnich 3 lat przed terminem składania ofert:

- zrealizował co najmniej 2 projekty z zakresu opracowania systemu zarządzania cyberbezpieczeństwem dla przedsiębiorstw z branży automotive; (wymagane oświadczenie)
- zrealizował co najmniej 1 projekt z zakresu opracowania systemu zarządzania cyberbezpieczeństwem dla przedsiębiorstw z branży Bus & Trucks. (wymagane oświadczenie)

Osoby zdolne do wykonania zamówienia

Wykonawca dysponuje zespołem co najmniej 10 ekspertów z dziedziny zapewnienia cyberbezpieczeństwa pojazdom. Kwalifikacje zespołu są potwierdzone poprzez posiadane certyfikaty z obszaru cyberbezpieczeństwa w ilości co najmniej 10 szt.

(wymagane oświadczenie z załączoną listą certyfikatów zespołu)

Potencjał techniczny

Wykonawca dysponuje własnym zapleczem/ laboratorium do wykonywania testów penetracyjnych dedykowanym branży automotive znajdującym się na terenie Europy, działającym od co najmniej 1 roku. Zaplecze musi posiadać minimum:

- laboratorium do badania ECU (sterowników),
- niezbędny sprzęt i oprogramowanie do tworzenia i obsługi symulacji Restbus
- niezbędny sprzęt i oprogramowanie do łączenia, przechwytywania i pracy z kanałami komunikacyjnymi minimum CAN i Automotive Ethernet

(deklaracja, w razie konieczności dowód potwierdzający)

Na żądanie Zamawiającego wykonawca zobowiązany jest przedstawić wykaz realizacji, zawierający informację o: przedmiocie badań, dacie wykonania i podmiotach na rzecz których dostawy zostały wykonane, oraz potwierdzić należyte zrealizowanie tych dostaw odpowiednimi dokumentami.

Dokumentami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego dostawy były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy.

Zleceniodawca dopuszcza weryfikację efektów pracy (dokumentacji) przez firmę / organizację zewnętrzną. Weryfikacja może odbyć się etapami po zakończeniu prac na określonym dokumentem / analizą lub całościowo w ostatnim miesiącu projektu.

Warunkiem odbioru jest akceptacja dostarczony dokumentów / analiz przez firmę Solaris lub organizację zewnętrzną.

c. Zawarcie umowy

a. Istotne warunki zawarcia umowy:

- a) przekazanie praw własności intelektualnych do produktu na rzecz zamawiającego
- b) termin płatności – maksymalnie 60 dni po każdym etapie realizacji

b. Wykonawca, którego oferta zostanie oceniona jako najkorzystniejsza, zobowiązany jest do zawarcia umowy z Zamawiającym w terminie **do 14 dni kalendarzowych** od daty przesłania wzoru umowy lub niezwłocznie po uzyskaniu przez Zamawiającego zgody właściwej instytucji zarządzającej projektem (jeśli taka zgoda jest wymagana). Jeżeli wykonawca, którego oferta została wybrana jako najkorzystniejsza, będzie uchylał się od zawarcia umowy we wskazanym wyżej terminie, zostanie to uznane za odstąpienie wykonawcy od podpisania umowy z Zamawiającym. W takiej sytuacji Zamawiający ma prawo podpisać umowę z kolejnym wykonawcą, który w niniejszym postępowaniu uzyska kolejną najwyższą liczbę punktów w procedurze oceny ofert.

c. Zmiany w umowie:

1. Zakazuje się zmian istotnych postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, chyba że zachodzi co najmniej jedna z następujących okoliczności:

a) zmiana terminu realizacji przedmiotu umowy jest wynikiem wystąpienia okoliczności niezależnych od Wykonawcy, przy zachowaniu przez niego należytej staranności, skutkujących niemożnością dotrzymania terminu realizacji przedmiotu umowy;

b) zmiana terminu realizacji przedmiotu umowy jest wynikiem wystąpienia siły wyższej, skutkującej niemożnością dotrzymania terminu realizacji przedmiotu umowy;

c) zmiana nie prowadzi do zmiany charakteru umowy i zostały spełnione łącznie następujące warunki:

- konieczność zmiany umowy spowodowana jest okolicznościami, których Zamawiający, działając z należytą starannością, nie mógł przewidzieć,

- wartość zmiany nie przekracza 50% wartości zamówienia określonej pierwotnie w umowie;

d) wykonawcę, któremu Zamawiający udzielił zamówienia, ma zastąpić nowy wykonawca:

- w wyniku połączenia, podziału, przekształcenia, upadłości, restrukturyzacji lub nabycia dotychczasowego wykonawcy lub jego przedsiębiorstwa, o ile nowy wykonawca spełnia warunki udziału w postępowaniu, nie zachodzą wobec niego podstawy wykluczenia oraz nie pociąga to za sobą innych istotnych zmian umowy,

- w wyniku przejęcia przez Zamawiającego zobowiązań wykonawcy względem jego podwykonawców;

e) zmiana nie prowadzi do zmiany charakteru umowy a łączna wartość zmian jest mniejsza niż 215.000 EUR i jednocześnie jest mniejsza od 10% wartości zamówienia określonej pierwotnie w umowie.

2. Zmianę uznaje się za istotną jeżeli zmienia ogólny charakter umowy, w stosunku do charakteru umowy w pierwotnym brzmieniu albo nie zmienia ogólnego charakteru umowy i zachodzi co najmniej jedna z następujących okoliczności: zmiana wprowadza warunki, które,

gdyby były postawione w postępowaniu o udzielenie zamówienia, to w tym postępowaniu wzięliby lub mogliby wziąć udział inni wykonawcy lub przyjęto by oferty innej treści, zmiana narusza równowagę ekonomiczną umowy na korzyść wykonawcy w sposób nieprzewidziany pierwotnie w umowie, zmiana znacznie rozszerza lub zmniejsza zakres świadczeń i zobowiązań wynikający z umowy lub polega na zastąpieniu wykonawcy, któremu Zamawiający udzielił zamówienia, nowym wykonawcą, w przypadkach innych niż wymienione w pkt. 1 lit. d).

d. Opis sposobu przygotowania oferty:

- a. Wykonawca powinien przedstawić ofertę w języku polskim lub języku angielskim.
- b. Oferta powinna być rozbita wg pozycji przedstawionych w formularzu ofertowym.
- c. Oferta powinna być złożona na wypełnionym i podpisanym formularzu ofertowym, który stanowi załącznik do zapytania ofertowego.

Brak jakiegokolwiek z wyżej wymienionych elementów skutkować będzie odrzuceniem oferty z przyczyn formalnych.

e. Kryteria oceny ofert i opis sposobu przyznawania punktacji:

- a. Ocenie podlegają tylko oferty ważne, tj.:
 - i. złożone w terminie
 - ii. przygotowane zgodnie z wymogami określonymi w pkt. 7

- b. Kryteria oceny ofert:

Wybór oferty dokonany zostanie na podstawie oceny punktowej. Oferty niepodlegające odrzuceniu zostaną ocenione w oparciu o następujące kryteria i wagi procentowe:

Cena - waga kryterium 70%, maksymalna ilość punktów możliwych do uzyskania to 70.

$$P = (C_{\min} / C_{\text{obliczana}}) * P_{\max}$$

P – ilość zdobytych punktów przez oferenta

$C_{\min}$ – najniższa zaoferowana cena

$C_{\text{obliczana}}$ – cena zaproponowana przez oferenta

$P_{\max}$ – maksymalna liczba punktów do zdobycia

Cena podana w formularzu ofertowym – załącznik nr 1 do zapytania ofertowego – musi uwzględniać wszystkie koszty realizacji przyszłej umowy oraz musi wynikać z formularza ofertowego.

Ostateczna cena zadeklarowana w ofercie musi zawierać prawidłową stawkę podatku VAT.

Cenę ofertową należy podać w walucie polskiej (PLN), do dwóch miejsc po przecinku. Zamawiający dopuszcza możliwość podania ceny ofertowej w innej walucie niż PLN, przez Wykonawcę mającego siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej. W przypadku złożenia oferty w innej walucie niż PLN, zamawiający na potrzeby oceny ofert dokona przeliczenia tej waluty na PLN wg średniego bieżącego kursu wyliczonego i ogłoszonego przez Narodowy Bank Polski z dnia wszczęcia niniejszego postępowania (tj. z dnia upublicznienia zapytania ofertowego).

Poza cenowe kryteria oceny oferty:

Ilość zrealizowanych projektów z obszaru zarządzania cyberbezpieczeństwem w branży bus/trucks w firmach powyżej 1000 pracowników

- Brak – 0 punktów
- 1 zrealizowany projekt – 5 punktów
- 2 lub więcej – 10 punktów

(na podstawie oświadczenia wraz z ogólnym opisem zrealizowanych projektów)

Liczba certyfikatów i dokumentów równoważnych z obszaru cyberbezpieczeństwa posiadanych przez dostępny zespół ekspertów. (np. dyplom ukończenia studiów, szkolenia itp., należy wymienić.)

- Od 0 do 10 – 0 punktów
- od 11 do 25 – 10 punktów
- 26 lub więcej - 20 punktów

(na podstawie listy)

Maksymalna liczba punktów możliwych do uzyskania to 100 pkt.

Oferta, która otrzyma największą liczbę punktów wyliczoną zgodnie z powyższymi zasadami, zostanie uznana za najkorzystniejszą.

O wyborze najkorzystniejszej oferty Zamawiający zawiadomi wykonawców elektronicznie na adres e-mail, z którego została przesłana oferta albo na adres email wskazany w ofercie.

Zamawiający opublikuje informacje o wyniku niniejszego postępowania ofertowego na stronie internetowej: www.bazakonkurencyjności.gov.pl

f. Pozostałe informacje:

- a. Do upływu terminu składania ofert Zamawiający zastrzega sobie prawo zmiany lub uzupełnienia treści niniejszego zapytania ofertowego lub jego załączników. Jeżeli zmiany będą miały wpływ na treść składanych w postępowaniu ofert Zamawiający przedłuży termin składania ofert. Dokonane zmiany zostaną przekazane niezwłocznie wszystkim wykonawcom, do których zostało przekazane zapytanie ofertowe i będą one dla nich wiążące.
- b. Zamawiający zastrzega sobie prawo do poprawienia w treści otrzymanych ofert oczywistych omyłek pisarskich lub rachunkowych oraz innych omyłek polegających na niezgodności oferty z zapytaniem ofertowym, niepowodujących istotnych zmian w treści oferty, niezwłocznie zawiadamiając o tym danego wykonawcę.
- c. Pytania dotyczące zapytania ofertowego należy kierować do Zamawiającego drogą elektroniczną na adres e-mail: zapytanie.projekt@solarisbus.com. Treść pytań dotyczących zapytania ofertowego wraz z wyjaśnieniami zamawiającego zostanie opublikowana na stronie

ogłoszenia zapytania ofertowego. Zamawiający zastrzega możliwość pozostawienia pytań bez odpowiedzi, jeżeli wpłyną one do Zamawiającego w przedostatnim dniu przed upływem terminu składania ofert.

- d. Zamawiający zastrzega sobie prawo do unieważnienia niniejszego postępowania bez podawania przyczyny, na każdym jego etapie do momentu wyboru oferty wykonawcy.
- e. W przypadku zakończenia postępowania bez wyboru którejkolwiek oferty, wykonawcom nie przysługuje żadne roszczenie w stosunku do Zamawiającego.
- f. Powyższe zapytanie nie stanowi oferty w rozumieniu Kodeksu cywilnego.

Załączniki:

- 1. Formularz ofertowy
- 2. Klauzula o przetwarzaniu danych osobowych
- 3. Oświadczenie o braku powiązań
- 4. Oświadczenie o spełnieniu wszystkich warunków udziału w postępowaniu