Główny Inspektorat Ochrony Środowiska

Inspekcji Ochrony Środowiska

Departament Informatyzacji

tel. + 48 22 36 92 329 e-mail: sekretariatdinf@gios.gov.pl ul. Bitwy Warszawskiej 1920 r. 3, 02–362 Warszawa

Warszawa, dnia: 27 lipca 2022 r.

DINF-SBT.26.4.2022

Zapytanie w sprawie rozeznania rynku na zamówienie

pt.: „Audyt bezpieczeństwa sieci i rozwiązań IT w GIOŚ"

Zamawiający - Główny Inspektorat Ochrony Środowiska, ul. Bitwy Warszawskiej 1920 r. 3, 02-362 Warszawa, zamierza wszcząć zamówienie publiczne na usługę przeprowadzenia audytu bezpieczeństwa sieci i rozwiązań IT na potrzeby Zamawiającego - Głównego Inspektoratu Ochrony Środowiska (w skr. GIOŚ), ul. Bitwy Warszawskiej 1920 r. nr.3, 02-362 Warszawa.

W związku z tym zwracamy się do potencjalnych Wykonawców o przedłożenie wstępnego oszacowania kosztów, terminu dostawy oraz czasu realizacji zamówienia.

Główny Inspektorat Ochrony Środowiska informuje, że niniejsze zapytanie nie stanowi oferty w rozumieniu art.66 Kodeksu Cywilnego, ani nie jest ogłoszeniem o zamówieniu w rozumieniu ustawy Prawo Zamówień Publicznych. Informacja ta ma na celu wyłącznie ustalenie wartości szacunkowej poszczególnych zadań. Ostateczny opis przedmiotu zamówienia może się różnić od przedstawionego poniżej.

Kod CPV: 72800000-8

Opis: Usługi audytu komputerowego i testowania komputerów

1. **Cel zamówienia:**

   Celem zamówienia będzie usługa **przeprowadzenia audytu bezpieczeństwa sieci i rozwiązań IT na potrzeby GIOŚ** w opisanym poniżej zakresie.

2. **Przewidywany zakres zamówienia:**

   Usługa będzie realizowana zdalnie i dotyczyć będzie całości adresacji IP sieci GIOŚ widocznej w sieci Internet oraz dostępów i segmentacji rozwiązań wewnątrz sieci WAN Zamawiającego, mającego główna siedzibę na ul. Bitwy Warszawskiej 1920 r. 3 w Warszawie i będzie obejmować:

a. Przeprowadzenie zewnętrznego (poprzez dostęp z sieci Internet) badania odporności rozwiązań ICT (technologii informatycznych i komunikacyjnych) Zamawiającego, na znane i potencjalne zagrożenia cyberbezpieczeństwa - to jest przeprowadzenie testów i wykonanie analiz ich wyników w zakresie widocznej w Internecie adresacji IP powiązanej z serwisami i usługami GIOŚ. Parametry w tym koszt i szczegółowy zakres usługi powinny zostać opisane modułowo w sposób umożliwiający dostosowanie zakresu do warunków i potrzeb Zamawiającego.
b. Przeprowadzenie w uzgodniony z Zamawiającym terminie wewnętrznego badania/testów bezpieczeństwa sieci WAN i rozwiązań teleinformatycznych GIOŚ, ze szczególnym uwzględnieniem odporności na potencjalna atak przeprowadzony z wewnątrz sieci po uzyskaniu dostępu w wyniku symulacji przeprowadzeniu „skutecznego ataku" z przejęciem uprawnień „zwykłego użytkownika" oraz użytkownika z „podwyższonymi uprawnieniami". Badanie powinno uwzględniać odporność rozwiązań Zamawiającego na: przejecie uprawnień do zarzadzania serwisami w sieci dla ich kompromitacji oraz na masowe zaszyfrowanie danych (ransomware), a także ocenić przygotowanie Zamawiającego do działań celem odzyskania utraconych w takim ataku danych.
c. Zamawiający wymaga przeprowadzenia niezbędnych testów i analiz opisanych powyżej, których wynikiem ma być „Raport podsumowujący" złożony z części badania odporności na cyberatak „z zewnątrz" i „wewnątrz" (Raport sporządzony jako „tajemnica przedsiębiorstwa") zawierający poza wynikami przeprowadzonego badania z wyszczególnieniem zakresu, sposobu i wyników poszczególnych testów, również informacje o poziomie (severity) wykrytych zagrożeń oraz działań zapobiegawczych zaleconych do natychmiastowego podjęcia (w uzgodnieniu z Zamawiającym), a także działań korygująco naprawczych oraz zaleceń w zakresie koniecznych do podjęcia samodzielnie przez Zamawiającego działań wzmacniających i rekonstrukcyjnych dla rozwiązań bezpieczeństwa ICT. Raport winien zawierać wstęp/skrót/podsumowanie o charakterze „jawnym". W zakresie wspomnianych zaleceń dotyczących działań korygująco naprawczych po przeprowadzonym badaniu w Raporcie musza się znaleźć opisy (instrukcje) samodzielnego wykonania wskazanych i opisanych działań przez administratorów Zamawiającego oraz zalecenia (sugerowane kierunki) rekonstrukcji i uzupełniania rozwiązań Zamawiającego dla podniesienia bezpieczeństwa ICT.
d. Po realizacji przez Zamawiającego zalecanych działań w związku z ew. wykrytymi zagrożeniami i zalecanymi działaniami korygująco naprawczymi, Wykonawca w każdym z zakresów (a i b) winien przeprowadzić niezwłocznie retesty, ujmując ich wyniki w Raporcie opisanym w pkt c.

Dodatkowe wymagania:

O zamówienie będzie mógł się ubiegać Wykonawca, który w ciągu ostatnich dwóch lat (w okresie od styczeń 2020r. do lipiec 2022r.) realizował podobne co do zakresu usługi badania cyberbezpieczeństwa na wskazanym przez Zamawiającego łącznym poziomie kwot tych zamówień. Ponadto Zamawiający zastrzega, że wszelkie prowadzone w ramach usługi testy nieinwazyjne mogą być realizowane w godzinach 8:00-16:00 pod warunkiem uzgodnienia wsparcia ze strony Zamawiającego. Testy o dużym prawdopodobieństwie zaburzenia funkcjonowania rozwiązań Zamawiającego muszą być prowadzone po godzinie 16:00 i optymalnie w dni wolne i powinny być szczegółowo uzgodnione z Zamawiającym.

3. **Termin składania szacunkowej ofert:**

   Szacunkowe oferty należy złożyć elektronicznie na adres oferty.dinf@gios.gov.pl
   do dnia 05-08-2022 r. do godziny 14:00,
   w formie opisu i/lub ew. uwag do zakresu wskazanego w niniejszym Zapytaniu.
   W ramach szacunkowej wyceny należy podać wartość netto, stawkę podatku VAT, wartość brutto wyrażone w polskich złotych. Wycena powinna obejmować wszystkie koszty związane z realizacją pełnego zakresu przedmiotu zamówienia i w miarę możliwości odnosić się do każdej ze wskazanych pozycji.

4. **Osoby wskazane do kontaktu:**

   Osoba uprawniona do kontaktu z potencjalnymi Wykonawcami:

(imię i nazwisko)	Jerzy Goraziński
(Wydział / Departament)	Departament Informatyzacji
(telefon)	22 396 22 98 w godzinach 9:00 – 15:00
(adres e-mail)	j.gorazinski@gios.gov.pl

Marcin Stalpiński
Dyrektor Departamentu

/podpisano kwalifikowanym podpisem elektronicznym/