ZAPYTANIE O SZACUNKOWĄ WARTOŚĆ ZAMÓWIENIA NA ŚWIADCZENIE USŁUG AUDYTÓW BEZPIECZEŃSTRWA ORAZ TESTÓW PENETRACYJNYCH SYSTEMÓW I INFRASTRUKTURY INFORMATYCZNEJ NCBR

Narodowe Centrum Badań i Rozwoju (NCBR), z siedzibą w Warszawie (00-695), przy ul. Nowogrodzkiej 47a (NIP: 701-007-37-77, REGON: 141032404) planuje wszczęcie postępowania o udzielenie zamówienia publicznego, którego przedmiotem będzie realizacja zamówienia na świadczenie usług audytów bezpieczeństwa oraz testów penetracyjnych systemów i infrastruktury informatycznej NCBR.

W związku z powyższym, **w celu oszacowania wartości zamówienia,** Zamawiający zwraca się z prośbą o udzielenie informacji na temat szacunkowego kosztu realizacji usługi.

I. Cel i przedmiot planowanego zamówienia

1. Przedmiotem zamówienia jest świadczenie usług:
   a) audyty bezpieczeństwa oraz testy penetracyjne systemów IT,
   b) audyty kodu źródłowego,
   c) audyty bezpieczeństwa oraz testy penetracyjne infrastruktury
2. Przedmiot zamówienia 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) w zakresie całej infrastruktury i wszystkich systemów NCBR.
   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.

II. Kod CVP:

72254100-1 - Usługi w zakresie testowania systemu

III. Opis przedmiotu zamówienia

1. 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
2. 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 niniejszego paragrafu 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.
3. Testy bezpieczeństwa i audyty kodu obejmować będą co najmniej następujące elementy:

Lp.	Nazwa usługi	Zakres
1	Audyt kodu aplikacji webowej	• Określenie powierzchni ataku • Określenie obszarów podwyższonego ryzyka • Określenie zgodności ze standardami organizacji • Identyfikacja klas podatności • Weryfikacja wdrożonych zaleceń
2	Test penetracyjny aplikacji	• Testy penetracyjne serwera WWW • Testy penetracyjne serwera aplikacyjnego • Testy penetracyjne aplikacji (komponenty dostępne publicznie) • Testy penetracyjne aplikacji po uwierzytelnieniu) • Testy penetracyjne interfejsów bazy danych • Testy penetracyjne bazy danych z poziomu użytkownika

3	Test penetracyjny sieci lokalnej	• Testy penetracyjne punktu styku z Internetem • Kontrolowana próba obejścia zabezpieczeń • Testy uwierzytelniania sieciowego • Testy szczelności VLANów i poufności przesyłanych informacji • Testy penetracyjne systemów operacyjnych

4. W ramach przyszłej realizacji Przedmiotu Umowy zostaną wykonane następujące badania bezpieczeństwa, zgodnie z poniższym opisem
    a) Ocena podatności - identyfikacja podatności występujących w systemach informatycznych, przy pomocy automatycznych narzędzi testujących. W przypadku tego typu badania nie występuje próba wykorzystania wykrytych podatności, w celu uzyskania dostępu do testowanych systemów.
    b) Test penetracyjny - określenie faktycznego stanu bezpieczeństwa polegające na symulacji prób złamania lub ominięcia zabezpieczeń. W trakcie testów stosowane są metody i narzędzia, którymi zwykle posługują się potencjalni napastnicy. Zidentyfikowane podatności są wykorzystywane do przejęcia kontroli nad testowanymi systemami oraz do dalszych prób eskalacji ataku. Umożliwia to określenie potencjalnej skali naruszenia bezpieczeństwa, która wystąpi, jeśli te podatności zostaną wykorzystane przez hackerów.
    c) Testy realizowane jako testy penetracyjne funkcjonalności dostępnych z zewnątrz oraz jako ocena podatności infrastruktury w obszarze funkcji dostępnych z sieci wewnętrznej.
5. Badania obejmą co najmniej podatności co najmniej na podatności wymienione w OWASP Top 10 (Most Critical Web Application Security Risks)
6. W ramach testów zostaną wykorzystane dwa rodzaje testów penetracyjnych: black box (z minimalną wiedzą o audytowanej aplikacji) oraz crystal box (z pełną wiedzą i kontem użytkownika w audytowanej aplikacji).
7. Testom bezpieczeństwa i audytom podlegać będą systemy informatyczne i aplikacje użytkowane przez Zamawiającego, zarówno zewnętrzne jak i wewnętrzne, funkcjonujące w określonym środowisku Zamawiającego.
8. Testom bezpieczeństwa podlegać będą systemy w przeważającej większości oparte o technologie: PHP, JSP/Java, Ruby on Rails, Python, Perl, ASP/ASP.NET.
9. Testy aplikacji w większości będą przeprowadzane na instancjach przeznaczonych do testowania (nieprodukcyjnych).
10. Testy mogą wymagać obecności Wykonawcy w siedzibie Zamawiającego.

W przypadku środowisk utrzymywanych w centrach danych partnerów zewnętrznych, Zamawiający każdorazowo zapewni zgodę operatora centrum danych na wykonanie testów.

Wykaz systemów Zamawiającego

Lp.	*Rodzaj audytu*	*Obszar*
1	Testy penetracyjne i ocena podatności oraz Audyt kodu aplikacji	Lokalny System Informatyczny – aplikacja do naboru i obsługi wniosków o dofinansowanie
2	Testy penetracyjne i ocena podatności	aplikacja „System do rejestrowania umów i przychodów z projektów”
3	Testy penetracyjne i ocena podatności	aplikacja ”Portal rejestracyjny dla ekspertów”
4	Testy penetracyjne i ocena podatności	witryna www
5	Testy penetracyjne i ocena podatności	aplikacja ”Portal ankiet”
6	Testy penetracyjne i ocena podatności	aplikacja ”System do naboru wniosków w konkursach międzynarodowych”
7	Testy penetracyjne i ocena podatności	system kadry-płace-finanse-księgowość
8	Testy penetracyjne i ocena podatności	system samoobsługi pracowniczej
9	Testy penetracyjne i ocena podatności	EZD - Elektroniczne Zarządzanie Dokumentacją
10	Testy penetracyjne i ocena podatności	infrastruktura Intranet
11	Testy penetracyjne i ocena podatności	styk z siecią Internet – OwnCloud
12	Testy penetracyjne i ocena podatności	styk z siecią Internet - Poczta e-mail – usługi MS Exchange Serwer plus OWA
13	Testy penetracyjne i ocena podatności	styk z siecią Internet
14	Ocena podatności	infrastruktura teleinformatyczna
15	Testy penetracyjne i ocena podatności	wskazane fragmenty sieci wewnętrznej
16	Raport z testów	udokumentowane wyniki prowadzonych badań audytowych
17	Retesty zakończone Raportem z retestów	ponowne testy całości badanego środowiska i aplikacji/systemów przeprowadzane po wprowadzeniu zmian, także tych wiążących się z wdrożeniem zaleceń poaudytowych

IV. Inne istotne informacje:

1). Wymagane doświadczenie Wykonawcy

1. O udzielenie przyszłego zamówienia będą mogli ubiegać się Wykonawcy, którzy:
   a) nie podlegają wykluczeniu,
   b) spełniają warunku udziału w postępowaniu w zakresie posiadania wiedzy i doświadczenia, tj. w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonali należycie, a w przypadku świadczeń okresowych lub ciągłych część wykonana obejmuje:
      i. co najmniej dwie usługi, w których w ramach każdej z nich wykonano co najmniej 40 roboczodni testów penetracyjnych typu black-box systemów informatycznych zawierających komponenty udostępniane publicznie w sieci Internet, z czego, co najmniej jedna usługa dotyczyła badania systemu, który był średniej wielkości (dla min. 200 użytkowników),
   c) spełniają warunki udziału w postępowaniu w zakresie dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia, tj.: co najmniej trzema ekspertami z których każdy:
      i. posiada co najmniej 3 letnie doświadczenie w wykonywaniu testów bezpieczeństwa systemów informatycznych i aplikacji webowych,
      ii. brał udział w co najmniej trzech usługach polegających łącznie na wykonaniu testów bezpieczeństwa systemów informatycznych średniej wielkości (dla min. 200 użytkowników), zawierających komponenty udostępniane publicznie w sieci Internet,

oraz

      iii. co najmniej jeden ekspert posiada certyfikat CISA - Certified Information Systems Auditor lub równoważny,
      iv. co najmniej jeden ekspert posiada certyfikat CISSP - Certified Information Systems Security Professional lub równoważny,

v. co najmniej jeden ekspert posiada certyfikat CEH (Certfied Ethical Hacker) lub CPTE (Certified Penetration Testing Engineer).

vi. co najmniej jeden ekspert posiada certyfikat Audytora Wiodącego lub Wewnętrznego ISO 27001 lub równoważny,

vii. co najmniej jeden ekspert posiada certyfikat Audytora Wiodącego lub Wewnętrznego ISO 20000 lub równoważny.

2) wymagania dotyczące warunków świadczenia usług

1. Wykonawca podejmie prace będące przedmiotem przyszłego Zamówienia w terminie 14 dni roboczych od daty złożenia Zamówienia przez Zamawiającego dla audytu pełnego, w terminie 3 dni roboczych dla audytu ad hoc.
2. Wykonawca wykona Zamówienia w terminie 14 dni roboczych od daty złożenia Zamówienia przez Zamawiającego dla audytu pełnego, w terminie 8 dni roboczych dla audytu ad hoc.
3. Terminy retestów dla każdego wykonanego Zamówienia będą ustalane przez Strony najpóźniej przed przekazaniem raportów z testów przez Wykonawca.

V. Miejsce oraz termin przedłożenia informacji o koszcie usług:

Drogą e-mailową na adres: **zamowienia-dsi@ncbr.gov.pl**, do dnia **6 czerwca 2018r**. do godziny **17:00**

VI. Informacje dodatkowe:

1. Wycena powinna obejmować pełny zakres prac określonych w zapytaniu oraz uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia.
2. Złożenie zapytania o szacunkowy koszt, jak też otrzymanie w jego wyniku odpowiedzi nie jest równoznaczne z udzieleniem zamówienia przez Narodowe Centrum Badań i Rozwoju (nie rodzi skutków w postaci zawarcia umowy).
3. Powyższe zapytanie nie stanowi oferty w rozumieniu Kodeksu cywilnego.
4. Zamawiający zastrzega sobie prawo do unieważnienia zapytania bez podania przyczyny oraz możliwość prowadzenia korespondencji celem doprecyzowania / wyjaśnienia treści złożonych odpowiedzi.
5. Wycena powinna być wyrażona w złotych polskich z uwzględnieniem należnego podatku VAT. Wycenę należy podać z dokładnością do dwóch miejsc po przecinku (zł/gr).
6. Wycena powinna być złożona na poniższym formularzu szacunkowej wyceny.

FORMULARZ SZACUNKOWEJ WYCENY

PEŁNA NAZWA WYKONAWCY: .....

ADRES Z KODEM POCZTOWYM: .....

TELEFON: .....

FAKS: .....

ADRES E-MAIL: .....

NUMER NIP:……..…….....

NUMER REGON: .....

Wycena realizacji świadczenia usług audytów bezpieczeństwa oraz testów penetracyjnych systemów i infrastruktury informatycznej NCBR

a) Cena za wykonanie jednego pełnego audytu bezpieczeństwa (raz w roku)
netto: …… zł
brutto: ……..… zł

b) Cena za wykonanie jednego audytu bezpieczeństwa ad hoc (maksimum 7 zamówień w roku)
netto: …… zł
brutto: ……..… zł

c) Maksymalna łączna wartość umowy obejmująca: dwa audyty pełne oraz maksymalnie 14 audytów ad hoc:
netto: …… zł
brutto: ……..… zł

Oświadczamy, że:

1) Nie wnosimy żadnych zastrzeżeń do zapytania o szacunkową wartość.
2) Przedłożona przez nas wycena obejmuje wszelkie koszty wykonania przyszłego zamówienia o udzielenie zamówienia publicznego.

……
miejscowość, data

…….
podpis, imię i nazwisko
lub podpis na pieczęci imiennej