Załącznik nr 2 do zapytania ofertowego

Znak sprawy: **BAF-WSLZP.26.74.2026**

OPIS PRZEDMIOTU ZAMÓWIENIA

Nazwa zamówienia: **Usługa diagnostyczno-analityczna w zakresie dostosowania Urzędu Państwowej Komisji do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15 do wymagań ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.) i dyrektywy (UE) 2022/2555 (NIS2)**, zrealizowana w terminie od dnia zawarcia umowy do 21 grudnia 2026 roku.

1. Przedmiot i cel. Usługa diagnostyczno-analityczna w zakresie dostosowania Urzędu do wymagań ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm., dalej „ustawa o KSC") i dyrektywy NIS2: ocena stanu obecnego (gap analysis), identyfikacja luk i ryzyk, przygotowanie podstaw do zaplanowania dalszych działań dostosowawczych oraz projektów i wzorów dokumentów systemu zarządzania bezpieczeństwem informacji (SZBI). Usługa nie stanowi audytu, o którym mowa w art. 15 ustawy o KSC, ani wdrożenia SZBI; przyjęcie i wdrożenie projektów i wzorów należy do Urzędu.

2. Informacje o Urzędzie i środowisku IT. Urząd jest podmiotem kluczowym w rozumieniu ustawy o KSC, wpisanym do wykazu prowadzonego na podstawie tej ustawy, i korzysta z systemu S46. Jedna lokalizacja (Warszawa, ul. Twarda 18); ok. 65–70 pracowników i współpracowników, 57 użytkowników systemów IT. Środowisko hybrydowe: 149 stacji roboczych, 44 serwery wirtualne, 3 węzły VxRail (vSphere), drugie środowisko wirtualizacyjne (3 serwery i macierz), serwer i repozytorium kopii zapasowych, Data Domain, 27 aktywnych urządzeń sieciowych, segmentacja VLAN; Microsoft 365 E5 (jeden tenant). Urząd nie posiada sformalizowanego SZBI; zarządzanie ryzykiem jest prowadzone wyłącznie w zakresie ochrony danych osobowych. W ostatnich 24 miesiącach nie przeprowadzano pełnych audytów, testów penetracyjnych ani ocen zgodności. Na początku realizacji zamówienia Urząd udostępni wykonawcy regulacje wprowadzone Zarządzeniem nr 1/2024 z dnia 8 stycznia 2024 r. (Polityka ochrony danych osobowych, Instrukcja użytkowania systemu informatycznego, Regulamin zarządzania systemem monitoringu wizyjnego), prowadzone rejestry, w tym rejestr naruszeń ochrony danych osobowych, oraz pozostałe posiadane dokumenty.

3. Zakres prac.

1. Weryfikacja obowiązków wynikających z ustawy o KSC dotyczących Urzędu jako podmiotu kluczowego, w tym terminów ich realizacji, oraz ocena aktualnego stanu: dokumentacji (w tym regulacji wprowadzonych Zarządzeniem nr 1/2024, ze wskazaniem, co zachować, co zmienić i co uzupełnić), procesów, systemów, zabezpieczeń organizacyjnych i technicznych.
2. Identyfikacja kluczowych zasobów, ich właścicieli i zależności, w tym zależności od dostawców i usług zewnętrznych (m.in. Microsoft 365, EZD RP, Enova, Płatnik), oraz ocena potrzeb w zakresie ciągłości działania.
3. Analiza luk i ryzyka na podstawie zweryfikowanych informacji i dowodów, z oceną istniejących zabezpieczeń i wskazaniem najistotniejszych ryzyk. Wykonawca rozwija metodykę określoną

w procedurze zarządzania ryzykiem zawartej w Polityce ochrony danych osobowych Urzędu tak, aby obejmowała wszystkie systemy i usługi Urzędu, oraz proponuje kryteria akceptacji ryzyka możliwe do dalszego stosowania przez Urząd.

4. Rekomendacje oraz plan dalszych działań z priorytetami, orientacyjnymi kosztami i podziałem na zadania własne Urzędu i wymagające wsparcia zewnętrznego.
5. Neutralne technologicznie wymagania dla dalszych działań w formie projektu opisu przedmiotu zamówienia wraz z szacunkową pracochłonnością.
6. Przegląd konfiguracji bezpieczeństwa środowiska Microsoft 365 E5 (m.in. Secure Score, uwierzytelnianie wieloskładnikowe, zasady dostępu warunkowego, rejestrowanie zdarzeń) w trybie tylko do odczytu, bez testów aktywnych.
7. Opracowanie projektów i wzorów dokumentów określonych w pkt 6.1 ppkt 7–10.
8. Prezentacja wyników kierownictwu Urzędu (w siedzibie lub zdalnie, do 2 godzin) oraz szkolenie dla kierownictwa Urzędu (w siedzibie, do 3 godzin) z obowiązków i odpowiedzialności kierownictwa wynikających z ustawy o KSC, z wykorzystaniem wyników usługi.
9. Wykonanie rezultatów dodatkowych określonych w pkt 6.2 – jeżeli wykonawca zaoferował je w ofercie.

4. Podstawy oceny. Ustawa o KSC wraz z aktami wykonawczymi, dyrektywa NIS2, rozporządzenie w sprawie Krajowych Ram Interoperacyjności w zakresie bezpieczeństwa informacji, RODO; pomocniczo normy PN-EN ISO/IEC 27001, ISO/IEC 27005 i ISO 22301.

5. Sposób realizacji. Analiza dokumentacji, wywiady z kierownictwem, IT i właścicielami procesów, przegląd wybranych ustawień i rejestrów udostępnionych przez Urząd (bez testów aktywnych), obserwacja w siedzibie. Część czynności może być realizowana zdalnie. Usługa nie obejmuje informacji niejawnych ani wglądu w treść akt spraw prowadzonych przez Departament Postępowań Wyjaśniających.

6. Rezultaty.

6.1. Rezultaty obowiązkowe:

1) raport z przeprowadzonych prac, zawierający co najmniej: opis zakresu, metodyki i ograniczeń, ustalenia dotyczące statusu Urzędu i jego obowiązków wynikających z ustawy o KSC wraz z podstawą prawną, ocenę stanu obecnego w poszczególnych obszarach, wykaz kluczowych zasobów i zależności, wnioski z analizy luk i ryzyka oraz podsumowanie dla kierownictwa;
2) macierz zgodności, obejmująca co najmniej obszary środków zarządzania ryzykiem wymienione w art. 21 ust. 2 lit. a–j dyrektywy NIS2 i odpowiadające im przepisy ustawy o KSC, w której dla każdego wymagania wskazano co najmniej: źródło wymagania (przepis ustawy o KSC, aktu wykonawczego lub dyrektywy NIS2), opis stanu stwierdzonego, odniesienie do dowodu, ocenę zgodności według przyjętej skali oraz zidentyfikowaną lukę;
3) rejestr luk i ryzyk zawierający opis metodyki i kryteriów oceny ryzyka (w tym kryteriów akceptacji), a dla każdej pozycji: identyfikator, opis, powiązane zasoby, prawdopodobieństwo, skutek, poziom ryzyka, proponowanego właściciela oraz rekomendowany sposób postępowania;
4) plan dalszych działań, w którym każde działanie zawiera: identyfikator powiązanej luki lub ryzyka, priorytet, proponowaną kolejność i termin, orientacyjny koszt lub pracochłonność, wskazanie, czy

zadanie może zostać wykonane zasobami własnymi Urzędu, czy wymaga wsparcia zewnętrznego, oraz odniesienie do ustaleń i dowodów;

5) neutralne technologicznie wymagania dla dalszych działań w formie projektu opisu przedmiotu zamówienia dla dalszych działań dostosowawczych, wraz z szacunkową pracochłonnością;

6) prezentacja wyników oraz materiały ze szkolenia dla kierownictwa Urzędu, obejmującego obowiązki i odpowiedzialność kierownictwa wynikające z ustawy o KSC;

7) projekt procedury obsługi i zgłaszania incydentów, zintegrowanej z procedurą zgłaszania incydentów określoną w Polityce ochrony danych osobowych Urzędu, obejmującej co najmniej: klasyfikację incydentów, w tym kryteria incydentu poważnego, role i zastępstwa, ścieżkę zgłoszeń do właściwego zespołu CSIRT za pośrednictwem systemu S46 w terminach określonych w ustawie o KSC, wzór karty zgłoszenia oraz wzór rejestru incydentów;

8) projekt polityki bezpieczeństwa informacji Urzędu jako dokumentu nadrzędnego systemu zarządzania bezpieczeństwem informacji, spójnego z regulacjami wprowadzonymi Zarządzeniem nr 1/2024 z dnia 8 stycznia 2024 r.;

9) pakiet wzorów dokumentów systemu zarządzania bezpieczeństwem informacji wraz z instrukcją ich wypełnienia, obejmujący co najmniej: plan ciągłości działania, plan odtwarzania po awarii, politykę kopii zapasowych z zasadami testów odtwarzania, politykę kontroli dostępu z zasadami uwierzytelniania wieloskładnikowego, politykę stosowania kryptografii, procedurę zarządzania podatnościami, aktualizacjami i zmianami, rejestr aktywów, rejestr ryzyk, plan postępowania z ryzykiem oraz deklarację stosowania;

10) pakiet dotyczący bezpieczeństwa łańcucha dostaw, obejmujący: wzór klauzul dotyczących cyberbezpieczeństwa do stosowania przy zakupie produktów ICT, usług ICT i procesów ICT, kwestionariusz oceny dostawcy oraz wzór oświadczenia dotyczącego dostawców wysokiego ryzyka;

11) raport z przeglądu konfiguracji bezpieczeństwa środowiska Microsoft 365, przeprowadzonego w trybie tylko do odczytu, bez testów aktywnych, zawierający listę działań usprawniających możliwych do wykonania zasobami własnymi Urzędu.

6.2. Rezultaty dodatkowe – jeżeli wykonawca zaoferował je w ofercie (kryterium „Dodatkowe rezultaty”):

1) scenariusz, przeprowadzenie i raport z ćwiczenia sztabowego (około 2 godzin) na scenariuszu ataku ransomware, weryfikującego projekt procedury, o której mowa w pkt 6.1 ppkt 7, wraz z rekomendacjami jej zmian; ćwiczenie odbywa się w siedzibie Urzędu po przekazaniu projektu procedury;

2) projekt zarządzenia aktualizującego Zarządzenie nr 1/2024 wraz z macierzą ról i odpowiedzialności, obejmującą co najmniej pełnomocnika do spraw cyberbezpieczeństwa, osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa, inspektora ochrony danych i komórkę odpowiedzialną za IT;

3) materiały szkoleniowe dla pracowników Urzędu z zakresu cyberbezpieczeństwa, obejmujące prezentację i test wiedzy z kluczem odpowiedzi, przeznaczone do samodzielnego wykorzystania przez Urząd.

6.3. Wymagania wspólne dla rezultatów:

1) każde ustalenie powinno być powiązane z dowodem (dokumentem, notatką z wywiadu, zrzutem lub zapisem konfiguracji udostępnionym przez Urząd albo wynikiem obserwacji); ustalenia oparte wyłącznie na deklaracjach, bez weryfikacji, oznacza się wyraźnie;

2) wymagania dla dalszych działań nie mogą wskazywać znaków towarowych, patentów, pochodzenia, producentów ani konkretnych produktów; jeżeli w wyjątkowych przypadkach jest to niezbędne, wykonawca uzasadnia to i dodaje wyrazy „lub równoważne" wraz z kryteriami równoważności;

3) projekty dokumentów (pkt 6.1 ppkt 7 i 8, pkt 6.2 ppkt 2) dostosowuje się do organizacji Urzędu i obowiązujących w nim regulacji; wzory (pkt 6.1 ppkt 9 i 10) mają charakter ogólny i zawierają instrukcję wypełnienia;

4) rezultaty nie mogą zawierać fragmentów norm ani innych utworów osób trzecich, do których wykonawca nie posiada praw umożliwiających przeniesienie autorskich praw majątkowych lub udzielenie licencji;

5) rezultaty sporządza się w języku polskim, w formacie PDF oraz w formatach edytowalnych (DOCX, XLSX, PPTX lub równoważnych), bez zabezpieczeń uniemożliwiających edycję; rejestr luk i ryzyk, macierz zgodności oraz plan działań przekazuje się dodatkowo w formacie arkusza kalkulacyjnego;

6) rezultaty przekazuje się kanałem zapewniającym szyfrowanie, uzgodnionym z Urzędem, i oznacza klauzulą „Informacja chroniona – do użytku wewnętrznego Urzędu".

7. Termin i warunki realizacji.

1) termin realizacji: do dnia 21 grudnia 2026 r.;

2) w terminie 3 dni roboczych od rozpoczęcia realizacji wykonawca przekazuje Urzędowi do akceptacji plan i harmonogram prac (lista wywiadów, wykaz potrzebnych dokumentów i informacji, metodyka analizy ryzyka, terminy przekazania projektów rezultatów); spotkanie otwierające z udziałem kierownictwa Urzędu odbywa się w terminie 5 dni roboczych od rozpoczęcia realizacji;

3) projekty wszystkich rezultatów wykonawca przekazuje nie później niż 5 dni roboczych przed upływem terminu realizacji; Urząd zgłasza uwagi w terminie 3 dni roboczych, a wykonawca uwzględnia je w wersji ostatecznej albo uzasadnia ich nieuwzględnienie;

4) szkolenie dla kierownictwa i ćwiczenie sztabowe (jeżeli zaoferowane) odbywają się w siedzibie Urzędu przed upływem terminu realizacji; ćwiczenie odbywa się po przekazaniu projektu procedury, o której mowa w pkt 6.1 ppkt 7;

5) odbiór następuje protokołem, po sprawdzeniu kompletności i zgodności rezultatów z niniejszym opisem; wynagrodzenie jest płatne po podpisaniu protokołu odbioru;

6) wykonawca przenosi na Urząd, w ramach wynagrodzenia, autorskie prawa majątkowe do rezultatów, w tym prawo do wprowadzania zmian i udostępniania rezultatów wykonawcom przyszłych zamówień;

7) wykonawca zachowuje w poufności informacje uzyskane w związku z realizacją zamówienia; dostęp do systemów Urzędu jest możliwy wyłącznie w trybie tylko do odczytu, na imiennych kontach z uwierzytelnianiem wieloskładnikowym; przetwarzanie danych osobowych odbywa się na podstawie powierzenia zgodnego z art. 28 RODO.