

Poland-Warsaw: Systems and technical consultancy services

OJ S 193/2023 06/10/2023

Contract notice

Services

Directive 2009/81/EC

Section I: Contracting authority/entity

I.1. Name and addresses

Official name: Zakład Ubezpieczeń Społecznych

Postal address: ul. Szamocka 3, 5

Town: Warszawa

Postal code: 01-478

Country: Poland

Contact person: Departament Zamówień Publicznych

E-mail: SekretariatDZP@zus.pl

Internet address(es):

General address of the contracting authority/entity: <https://www.zus.pl>

Address of the buyer profile: <https://www.zus.pl>

Electronic access to information: <https://portal.smartpzp.pl/zus/>

Electronic submission of tenders and requests to participate: <https://portal.smartpzp.pl/zus/>

Additional information can be obtained from:

the abovementioned address

Specifications and additional documents (including documents for competitive dialogue and a dynamic purchasing system) can be obtained from:

the abovementioned address

Tenders or requests to participate must be submitted: the abovementioned address

I.2. Type of the contracting authority

Body governed by public law

I.3. Main activity

Other: realizacja zadań z zakresu ubezpieczeń społecznych

I.4. Contract award on behalf of other contracting authorities/entities

The contracting authority is purchasing on behalf of other contracting authorities: no

Section II: Object of the contract

II.1. Description

II.1.1. Title attributed to the contract by the contracting authority

Świadczenie usług wsparcia eksploatacji i utrzymania Systemu Bezpieczeństwa Teleinformatycznego ZUS

II.1.2. Type of contract and place of performance or delivery

Services

Service category No 26: Other services

Main site or place of performance: ZUS

NUTS code PL911 Miasto Warszawa

II.1.3. Information about framework agreement

II.1.4. Information about framework agreement

II.1.5. Short description of the contract or purchase(s)

Zamawiający informuje, że poniżej przedstawia jedynie podstawowe informacje o zakresie zamówienia na Świadczenie usług wsparcia eksploatacji i utrzymania Systemu Bezpieczeństwa Teleinformatycznego ZUS". Informacje te mają charakter wstępny, informacyjny. Opis przedmiotu zamówienia odpowiadający wymaganiom art. 400 ustawy Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605), zwana dalej "ustawa Pzp", będzie stanowił element SWZ i zostanie przekazany Wykonawcom wraz z zaproszeniem do składania ofert zgodnie z art. 411 ust. 2 ustawy Pzp.

CZĘŚĆ I - PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia w zakresie wsparcia eksploatacji i utrzymania posiadanego przez Zamawiającego Systemu Bezpieczeństwa Teleinformatycznego Zakładu Ubezpieczeń Społecznych (dalej: SBT ZUS) jest świadczenie w szczególności następujących Usług:

- 1) Utrzymanie wskazanych Usług aplikacyjnych IT, Usług Narzędzi i Procesów zarządzania w Środowisku produkcyjnym w zakresie i na zasadach określonych w Metrykach Usług Wykonawcy.
- 2) Świadczenie Usług serwisowych oraz Konsultacji utrzymaniowych;
- 3) Pełnienie roli Integratora Bezpieczeństwa w zakresie i na zasadach określonych poniżej oraz innych wskazanych ról przy wdrażaniu zmian w SBT ZUS, zgodnie z Procedurami eksploatacyjnymi oraz Standardami IT ZUS;
- 4) Świadczenie Usług dodatkowych, obejmujących w szczególności:
 - a) dostosowanie SBT ZUS do zmian organizacyjnych Zamawiającego,
 - b) dostosowanie SBT ZUS do zmian Usług IT lub Standardów IT ZUS,
 - c) wsparcie w realizacji zadań wynikających ze zmian legislacyjnych,
 - d) dodatkowe wsparcie wdrożeniowe dla Usług IT i wsparcie powdrożeniowe dla Usług IT,
 - e) opracowanie dokumentacji w szczególności: projektowej, eksploatacyjnej, powykonawczej, analitycznej i raportowej etc.,
 - f) analiza, rozwój oraz utrzymanie wskazanych obszarów architektury IT Zamawiającego,
 - g) analiza i rekomendacje dotyczące architektury IT Zamawiającego w zakresie bezpieczeństwa teleinformatycznego Zamawiającego,
 - h) analiza i rekomendacje w zakresie planowanych wdrożeń i ich wpływu na SBT ZUS oraz poziom bezpieczeństwa Zamawiającego,
 - i) analiza i rekomendacje w zakresie budowy kanałów komunikacji z podmiotami zewnętrznymi i ich wpływu na poziom bezpieczeństwa teleinformatycznego Zamawiającego.

1.1 Usługi

Wsparcie udzielane przez Wykonawcę świadczone będzie w zakresie i na poziomie opisanym w Metrykach Usług Wykonawcy. Metryka Usługi Wykonawcy będzie stanowiła dokument określający zakres zobowiązań Wykonawcy oraz warunki realizacji tych zobowiązań.

Poziom dotrzymania przez Wykonawcę parametrów usługi (SLA) wynikający z Metryk Usług Wykonawcy będzie mierzony i rozliczany przez Zamawiającego i dostarczany przez Zamawiającego w formie raportu z poziomu świadczenia usług. Przygotowanie mechanizmów mierzących i rozliczających poziom dotrzymywanych przez Wykonawcę parametrów jest po stronie Zamawiającego. Dla Metryk Usług Wykonawcy rozliczanie poziomów świadczonych usług realizowane jest poprzez parametry Usługi utrzymania tj. dostępność, niezawodność, ciągłość, wydajność. Uzyskane wartości parametrów pozyskiwane są z Systemu Monitorowania Usług Zamawiającego (SMU) .

Celem zdefiniowania parametrów Usługi utrzymania jest zapewnienie poziomu świadczonych

przez Wykonawcę usług na poziomie nie niższym niż określony wartościami tych parametrów. Każdy z parametrów ma ustalone wartości gwarantowane, tzn. takie, które określają najniższy dopuszczalny przez Zamawiającego poziom, na jakim usługa może być świadczona. Ten poziom powinien gwarantować sprawną realizację procesów systemów. Komunikacja między Wykonawcą a Zamawiającym w zakresie obsługi i diagnozowania Incydentów, docelowo będzie odbywać się poprzez integrację Systemu obsługi Zgłoszeń Wykonawcy z Systemem obsługi Zgłoszeń Zamawiającego. Opis komunikacji i integracji będzie opisany w SWZ.

Zakres odpowiedzialności Wykonawcy

Wykonawca jest zobowiązany w szczególności do:

1. Świadczenia Usług utrzymania na poziomie określonym w Umowie zgodnie z wykorzystaniem zdefiniowanych przez Wykonawcę Procedur administracyjnych zatwierdzonych przez Zamawiającego lub posiadanych przez Zamawiającego.
2. Zapewnienia dotrzymania określonych w metrykach Parametrów świadczenia Usługi utrzymania.
3. Administrowanie i konfiguracja SBT ZUS, w tym udzielania Zamawiającemu niezbędnych zaleceń, wskazówek i wytycznych dotyczących eksploatacji Infrastruktury sprzętowo-systemowej wspierającej SBT ZUS objętego Metrykami Usług Wykonawcy.
4. Świadczenia Usług serwisowych w tym usuwania problemów wynikających z nieprawidłowego działania systemów objętych Metrykami Usług Wykonawcy.
5. Dostarczania Zamawiającemu informacji o wszystkich aktualizacjach zaoferowanych i wspieranych przez producenta wersji systemów objętych Metrykami Usług Wykonawcy, z zapewnieniem asysty przy ich implementacji w środowisku Zamawiającego. Wykonawca ustala z Zamawiającym czas instalacji dostarczonej aktualizacji systemów, przy czym Zamawiający będzie podejmował ostateczną decyzję o jej instalacji (Zamawiający w asyście Wykonawcy będzie dokonywał aktualizacji Oprogramowania, chyba że Strony postanowią inaczej).
6. Aktualizowania Dokumentacji w wyniku dostępności nowych wersji systemów oraz wprowadzanych poprawek.

1.1.1 Usługi utrzymania

Planowane są następujące usługi utrzymania:

Kategoria usługi Wykonawcy; Identyfikator usługi; Nazwa usługi;

Usługa utrzymania aplikacyjna SBT _ PAM Utrzymanie Systemu Bezpieczeństwa

Teleinformatycznego w zakresie zabezpieczenia dostępu do infrastruktury Zamawiającego

Usługa utrzymania aplikacyjna SBT _END Utrzymanie Systemu Bezpieczeństwa

Teleinformatycznego w zakresie zabezpieczenia stacji roboczych, poczty

Usługa utrzymania aplikacyjna SBT _DLP Utrzymanie Systemu Bezpieczeństwa

Teleinformatycznego w zakresie ochrony organizacji przed wyciekiem informacji

Usługa utrzymania aplikacyjna SBT _UTS_ INC Utrzymanie Systemu Bezpieczeństwa

Teleinformatycznego w obszarze incydentów bezpieczeństwa informacji

Usługa utrzymania aplikacyjna SBT _UTS_ TAG Utrzymanie Systemu Bezpieczeństwa

Teleinformatycznego w zakresie aplikacji do tagowania i szyfrowania

Usługa utrzymania –narzędzi i procesów zarządzania IT SBT _TEST_ KOD Badanie kodu

źródłowego – realizacja wg potrzeb Zamawiającego na zlecenie

Usługa utrzymania narzędzi i procesów zarządzania IT procesowa SBT _TEST_ PEN

Realizacja PENTEST – realizacja wg potrzeb Zamawiającego na zlecenie

Ostateczna lista Metryk Usług Wykonawcy zostanie ustalona w SWZ. Umowa będzie

zakładała możliwość dodawania nowych metryk w miarę potrzeb Zamawiającego

wynikających np. z rozwoju SBT ZUS.

A. Świadczenie utrzymania SBT ZUS

Celem świadczenia Usług utrzymania w zakresie określonym w Metrykach Usług Wykonawcy

jest zapewnienie produkcyjnego działania SBT ZUS we wdrożonych w ramach Umowy Ramowej, w tym również zapewnienie ich prawidłowego funkcjonowania w infrastrukturze systemowo-sprzętowej oraz ich integracji z innymi systemami zewnętrznymi.

Wykonawca w ramach usługi związanej z bieżącym utrzymaniem i wsparciem SBT ZUS odpowiedzialny będzie w szczególności za:

- a) bieżącą administrację SBT ZUS i bazami danych;
- b) identyfikację problemów oraz reagowanie na zidentyfikowane problemy i nieprawidłowości;
- c) rozwiązywanie problemów z działaniem systemów objętych metryką;
- d) rozwiązywanie problemów z działaniem agentów na stacjach roboczych Zamawiającego;
- e) wsparcie i asystę w aktualizacji oprogramowania systemowego na serwerach Zamawiającego;
- f) analizę i rekomendacje w zakresie strojenia baz danych na poziomie systemu operacyjnego /infrastruktury i ich realizację po udzielonej zgodzie Zamawiającego;
- g) rekomendacje dotyczące instalacji patchy i upgrade'ów (SBT ZUS i baz danych);
- h) realizację procedur administracyjnych;
- i) wykonywanie kopii bezpieczeństwa i ich testowanie;
- j) rekonfigurację SBT ZUS związanych z bieżącymi potrzebami środowiska i użytkowników;
- k) analizowanie i rekomendacje dotyczące podjęcia określonych działań oraz zmian koniecznych dla zapewnienia wysokiej wydajności SBT ZUS;
- l) informowanie o nowych wersjach SBT ZUS i przeprowadzanie na zlecenie Zamawiającego testów;
- m) uzgodnienia w zakresie harmonogramów aktualizacji SBT ZUS;
- n) aktualizację Dokumentacji SBT ZUS;
- o) weryfikację kompletności procedur administracyjnych, ich aktualizacja i uzupełnianie i tworzenie nowych;
- p) przygotowanie paczek instalacyjnych dla SCCM w zakresie instalacji/update agentów i asysta przy ich realizacji;
- q) przekazywanie raportów.

B. Zlecenie i realizacja testów bezpieczeństwa zdefiniowanych w ramach usług utrzymania SBT_TEST_KOD, SBT_TEST_PEN

Celem zlecenia testów w ramach metryk jest identyfikacja podatności stanowiących lub mogących stanowić zagrożenie dla bezpieczeństwa przetwarzanych, przesyłanych i przechowywanych informacji oraz danych, a także usług biznesowych realizowanych przez systemy teleinformatyczne Zamawiającego, których celem realizacji jest zaprojektowanie bezpiecznego środowiska teleinformatycznego w Zakładzie Ubezpieczeń Społecznych.

W zależności od potrzeb Zamawiający zleca testy w ramach metryk : SBT_TEST_KOD, SBT_TEST_PEN.

1. SBT_TEST_KOD

Badanie bezpieczeństwa kodu źródłowego to szczegółowa jego analiza, której celem jest odpowiedź na pytania, czy testowana aplikacja może być zainstalowana i wykorzystywana produkcyjnie, a także czy może być umieszczona w sieci, czy też mogą wiązać się z tym określone zagrożenia, a jeżeli tak, to jakie.

2. SBT_TEST_PEN

Test podatności aplikacji, systemów i sieci realizowany z sieci wewnętrznej i zewnętrznej jest badaniem umożliwiającym zbadanie odporności środowiska na atak będący efektem przełamania przez intruza zabezpieczeń na styku z sieciami zewnętrznymi, uzyskaniem przez intruza dostępu do wewnętrznej infrastruktury sieciowej albo celowego lub nieumyślnego działania legalnego użytkownika sieci (np. uruchomienie szkodliwego oprogramowania ze stacji roboczej użytkownika). Badanie to ma na celu wykrycie luk bezpieczeństwa oraz ich weryfikację pod kątem potencjalnych zagrożeń.

1.1.2 Usługi serwisowe

Zamawiający przewiduje następujące usługi serwisowe:

Usługa serwisowa SBT_ODI Obsługa Incydentów dotyczących Oprogramowania

Usługa serwisowa SBT_KON Konsultacje utrzymaniowe

A. Usługi serwisowe SBT_ODI – Obsługa Incydentów dotyczących Oprogramowania

Usługa obejmuje swym zakresem działania niezbędne do jak najszybszego przywrócenia poprawnego działania systemów, w tym: rejestrację Zgłoszenia, zidentyfikowanie przyczyn wystąpienia Incydentu, przekazanie wyników Diagnozy wraz z podaniem przyczyny Incydentu, dla Incydentów, dla których w wyniku Diagnozy stwierdzono konieczność dostarczenia Obejścia lub Rozwiązania, opracowanie i udostępnienie Obejścia i Rozwiązania lub opracowanie i udostępnienie Rozwiązania, w przypadku, gdy Obejście w procesie obsługi nie jest dostarczane, aktualizacja Dokumentacji, jeżeli zastosowane Obejście lub Rozwiązanie tego wymaga.

B. SBT_KON - Konsultacje utrzymaniowe

Usługa Konsultacji jest to wymiana informacji służących procesom rozwoju, integracji, zapewnienia ciągłości działania SBT ZUS oraz usuwania pojawiających awarii, realizowana pomiędzy Wykonawcą oraz Zamawiającym i innymi wykonawcami (świadczącymi usługi wsparcia w ramach innych umów z Zakładem w obszarze spoza SBT ZUS). Usługa Konsultacji utrzymaniowych nie ma na celu zlecenia wykonania prac analitycznych, projektowych lub programistycznych innym uczestnikom procesu Konsultacji, ani nie jest mechanizmem do transferu wiedzy ogólnej na temat SBT ZUS wynikającej z dokumentacji. Komunikacja w ramach Konsultacji pomiędzy Wykonawcami realizowana jest za pośrednictwem Zamawiającego.

1.1.3 Integrator Bezpieczeństwa – Pełnienie roli Integratora Bezpieczeństwa

Integrator Bezpieczeństwa wydaje opinie dot. wszystkich Modyfikacji, Usług dodatkowych oraz rozwiązań wdrażanych w ramach obsługi zgłoszeń serwisowych, których wdrożenie planowane jest we wszystkich oknach wdrożeniowych (planowanych oraz dodatkowych). Integrator Bezpieczeństwa bierze obowiązkowo udział w Konsultacjach ogólnych świadczonych przez wykonawców umów ramowych na rozwój Kompleksowego Systemu Informatycznego Zakładu Ubezpieczeń Społecznych.

Integrator Bezpieczeństwa współpracuje z Integratorem jako wykonawcą związanym umową, której przedmiotem są usługi wsparcia eksploatacji i utrzymania KSI ZUS.

A. Zadania Integratora Bezpieczeństwa w projektach SBT ZUS

a) Ocena wpływu na zasoby techniczne i usługi

Zadanie realizowane jest przez cały czas trwania każdego realizowanego projektu SBT ZUS (dalej zwanego „projektem”). Projekty mogą dotyczyć wszystkich wdrażanych zmian do systemów/funkcjonalności SBT ZUS a w szczególności Modyfikacji, Usług dodatkowych, naprawy zgłoszeń serwisowych oraz elementów na styku SBT ZUS z innymi systemami.

b) Udział w przygotowaniu produktów projektu/Produktów Innego wykonawcy, odbiorze oprogramowania i jego wdrożeniu

W ramach zadania Integrator Bezpieczeństwa uczestniczy w pracach Zespołu projektowego, testach akceptacyjnych oraz wykonuje testy regresji, międzymodułowe, wydajnościowe, bezpieczeństwa.

Zadaniem Integratora Bezpieczeństwa jest jednoznaczna ocena czy produkty projektu / Produkty Innego wykonawcy działają zgodnie z założeniami projektu i obowiązującymi standardami oraz potwierdzenie poprawności działania oprogramowania w Środowisku przedprodukcyjnym.

c) Rozpoczęcie eksploatacji i monitorowanie Okresu stabilizacji. Monitorowanie systemu w okresie utrzymania

W ramach zadania rolę Integratora Bezpieczeństwa jest jednoznaczna ocena czy produkty

projektu / Produkty Innego wykonawcy działają zgodnie z obowiązującymi Standardami eksploatacyjnymi. Integrator Bezpieczeństwa potwierdza poprawność działania oprogramowania w Środowisku produkcyjnym w Okresie stabilizacji oraz rekomenduje zakończenie Okresu stabilizacji.

d) Bieżące monitorowanie poziomu pojemności w kontekście utrzymania i rozwoju systemów bezpieczeństwa pozwalające na zaplanowanie i realizację przez Zamawiającego niezbędnych zakupów infrastrukturalnych

W ramach zadania rolą Integratora Bezpieczeństwa jest jednoznaczna ocena stanu pojemności i wydanie rekomendacji.

e) Identyfikacja potrzeb licencyjnych oraz bieżące monitorowanie poziomu wykorzystania licencji

Zadanie realizowane jest przez cały czas trwania każdego realizowanego projektu SBT (dalej zwanego „projektem”). Projekty mogą dotyczyć wszystkich wdrażanych zmian do systemów /funkcjonalności SBT ZUS a w szczególności Modyfikacji, Usług dodatkowych, naprawy zgłoszeń serwisowych oraz elementów na styku systemu SBT ZUS z innymi systemami. W ramach zadania rolą Integratora Bezpieczeństwa jest jednoznaczna ocena potrzeb licencyjnych i określenie czynności do realizacji.

B. Zadania Integratora Bezpieczeństwa w projektach/Planowanych zakupach realizowanych na styku SBT ZUS z innymi systemami

Ocena wpływu na zasoby techniczne i powiązane usługi

Zadanie realizowane jest przez cały czas trwania Umowy zgodnie z cyklem realizacji projektu wg ustalonego z Zamawiającym harmonogramem lub na żądanie, zgodnie z zapotrzebowaniem Zamawiającego.

W ramach zadania rolą Integratora Bezpieczeństwa jest identyfikacja ryzyk, wynikających z projektów/zapotrzebowania na zakupy w kontekście bezpieczeństwa, rekomendacja wymagań w zakresie zmian w konkretnych, będących w toku, projektach/zapotrzebowaniach na zakupy lub zastosowanie konkretnej architektury czy technologii pod względem bezpieczeństwa, oraz weryfikacja założeń projektowych, w tym założenia integracyjne, w kontekście możliwości realizacji oraz wpływ rozwiązań zaproponowanych w danych projektach na infrastrukturę techniczno-systemową SBT ZUS, w tym pojemność i ilość licencji SBT ZUS.

C. Zadania Integratora Bezpieczeństwa zapewniające bezpieczeństwo wdrożenia zmian Integrator Bezpieczeństwa ściśle współpracuje z Integratorem jako wykonawcą związanym umową, której przedmiotem są usługi wsparcia eksploatacji i utrzymania KSI ZUS. Integrator Bezpieczeństwa na bieżąco analizuje i opiniuje planowane do wdrożenia zmiany pod kątem bezpieczeństwa na podstawie przekazanych dokumentów.

D. Zadania dotyczące wsparcia w zakresie rozwoju i utrzymania architektury SBT ZUS Integrator Bezpieczeństwa świadczy wsparcie w zakresie rozwoju i utrzymania architektury IT w następującym zakresie:

1. Wsparcie w zarządzaniu zmianą w architekturze SBT ZUS w zakresie analizy czasowych i architektonicznych zależności między projektami SBT ZUS oraz między projektami SBT ZUS a projektami spoza SBT ZUS (na styku z SBT ZUS).

2. Wsparcie architektoniczne w zakresie analizy obecnego stanu architektury SBT ZUS.

3. Wsparcie architektoniczne w zakresie przeglądu architektury SBT ZUS i aktualizacja dokumentu opisującego architekturę SBT ZUS.

E. Udział Integratora Bezpieczeństwa w procesie rozwoju SBT ZUS oraz projektów będących na styku z SBT ZUS

1. Integrator Bezpieczeństwa zapewnia wsparcie Zamawiającemu w koordynowaniu rozbudowy/modyfikacji systemów informatycznych SBT ZUS.

2. Zadaniem Integratora Bezpieczeństwa jest ocena wpływu wdrożenia w Środowisku produkcyjnym produktów projektów/Produktów Innego wykonawcy realizowanych w ramach

umów rozwojowych na poziom bezpieczeństwa IT ZUS.

3. Integrator Bezpieczeństwa weryfikuje poprawność, spójność i integralność Kodów źródłowych oprogramowania w Środowisku przedprodukcyjnym Wykonawcy/Zamawiającego poprzez wykonanie procesu kompilacji.

4. Integrator Bezpieczeństwa współdziała z Zamawiającym w utrzymaniu i rozwoju metod walidacji Kodów źródłowych oprogramowania SBT ZUS.

1.2 Usługi dodatkowe

Zlecenia Usług dodatkowych mogą obejmować w szczególności wykonywanie prac w następującym zakresie:

- a) dostosowanie SBT ZUS do zmian organizacyjnych Zamawiającego,
- b) dostosowanie SBT ZUS do zmian Usług IT lub Standardów IT ZUS,
- c) wsparcie w realizacji zadań wynikających ze zmian legislacyjnych,
- d) dodatkowe wsparcie wdrożeniowe dla Usług IT i wsparcie powdrożeniowe dla Usług IT,
- e) opracowanie dokumentacji w szczególności: projektowej, eksploatacyjnej, powykonawczej, analitycznej i raportowej etc.,
- f) analiza, rozwój i utrzymanie architektury IT Zamawiającego,
- g) analiza i rekomendacje dotyczące architektury IT Zamawiającego w zakresie bezpieczeństwa teleinformatycznego Zamawiającego,
- h) analiza i rekomendacje w zakresie planowanych wdrożeń i ich wpływu na SBT ZUS oraz poziom bezpieczeństwa Zamawiającego,
- i) analiza i rekomendacje w zakresie budowy kanałów komunikacji z podmiotami zewnętrznymi i ich wpływu na poziom bezpieczeństwa teleinformatycznego Zamawiającego.

1.3 Warsztaty

Wykonawca jest zobowiązany do przeprowadzenia instruktaży przystanowiskowych m.in. w zakresie administrowania systemami i sprzętem objętych Usługami utrzymania, konfiguracji systemów, instalacji, wprowadzania zmian w konfiguracji, utrzymania, rozbudowy i modyfikacji baz i modernizacji systemów. Wykonawca przeprowadzi instruktaże dla wskazanych przez Zamawiającego osób.

Część II - OKRES PRZEJĘCIA USŁUG

Po zawarciu umowy Zamawiający umożliwi Wykonawcy zapoznanie z Elementami SBT ZUS oraz prześle stosowną dokumentację do zapoznania.

Przejęcie usług nastąpi w terminie określonym w SWZ.

1. Okres przekazywania usług kolejnemu Wykonawcy

1. Wykonawca zobowiązany jest do wsparcia Zamawiającego w przekazaniu Usług do Zamawiającego lub do nowego Wykonawcy.

2. Przewiduje się realizację Przekazania Usług w formie warsztatów/instruktaży.

Część III - OGÓLNY OPIS SYSTEMU BEZPIECZEŃSTWA TELEINFORMATYCZNEGO ZAKŁADU UBEZPIECZEŃ SPOŁECZNYCH

System Bezpieczeństwa Teleinformatycznego Zakładu Ubezpieczeń Społecznych (SBT ZUS) składa się z szeregu rozwiązań sprzętowo-technologicznych oraz oprogramowań podnoszących poziom bezpieczeństwa teleinformatycznego Zamawiającego.

Jego głównym obszarem działań jest zapewnienie zabezpieczenia poczty elektronicznej, dostępu do Internetu, stacji roboczych, sieci, tożsamości uprzywilejowanych.

SBT ZUS składa się z:

1. Stosu ICT dla systemów cyberbezpieczeństwa wraz z backupem - środowiska wirtualizacyjne oraz kopii zapasowej dla działających serwerów wirtualnych SBT ZUS.

2. Infrastruktury serwerowo-macierzowej zapewniającej połączenie sieciowe z resztą infrastruktury, oraz infrastrukturę dla systemu backupu danych, w szczególności:

- a) zapewnia infrastrukturę sieciowo-serwerową dla klastrów wirtualizacji oraz pozostałych systemów SBT ZUS;

- b) zapewnia możliwość połączenia systemów proxy z infrastrukturą Zamawiającego;
 - c) zapewnia możliwość połączenia systemów AntyAPT z infrastrukturą Zamawiającego.
 - 3. Urządzeń sieciowych i Firewall wraz z ich konfiguracją, oraz separacja środowisk zarządzających poszczególnych podsystemów.
 - 4. Systemów kategorii Network Visibility – infrastruktury składającej się z pojedynczej platformy packet broker oraz urządzeń typu aktywny TAP.
 - 5. Narzędzi zapobiegających wyciekom danych, na poziomie stacji końcowych, sieci, poczty elektronicznej oraz serwisów informacyjnych.
 - 6. Systemu klasy AntyAPT.
 - 7. Systemu klasy PAM pozwalającego na zarządzanie kontami uprzywilejowanymi.
 - 8. Aplikacji klasy Information Right Management, której podstawowe funkcjonalności to szyfrowanie plików, szyfrowanie wiadomości e-mail i/lub załączników, możliwość ograniczania uprawnień tylko do odczytu.
 - 9. Technologii kategoryzacji (klasyfikacji) informacji pozwalającą na podstawie zawartości pliku lub intencji użytkownika podzielić pliki na grupy, które podlegają regułom klasyfikacji.
- Wszystkie systemy są oprogramowaniem standardowym dostępnym na rynku.
Szczegółowy wykaz systemów oraz sprzętu składającego się na SBT ZUS pozwalającego na złożenie oferty zostanie ujawniony Wykonawcom wraz z SWZ.

II.1.6. CPV code(s)

72220000 Systems and technical consultancy services, 72230000 Custom software development services, 72250000 System and support services, 72253200 Systems support services

II.1.7. Information about subcontracting

The tenderer has to indicate in the tender any share of the contract it may intend to subcontract to third parties and any proposed subcontractor, as well as the subject-matter of the subcontracts for which they are proposed

The tenderer has to indicate any change occurring at the level of subcontractors during the execution of the contract

The contracting authority/entity may oblige the successful tenderer to award all or certain subcontracts through the procedure set out in Title III of Directive 2009/81/EC

II.1.8. Lots

This contract is divided into lots: no

II.1.9. Information about variants

Variants will be accepted: no

II.2. Scope of the procurement

II.2.1. Total quantity or scope

Umowa będzie zawarta na okres 60 miesięcy (w tym okres przejściowy - maksymalnie 3 miesiące).

Wstępny, informacyjny zakres zamówienia został określony w Sekcji II.1.5) Ogłoszenia, wartość zamówienia powyżej 431 000 EUR.

II.2.2. Information about options

Options: yes

Description of options: Zamawiający przewiduje prawo opcji, polegające na wydłużeniu okresu obowiązywania umowy o maksymalnie 9 miesięcy zgodnie z potrzebami Zamawiającego.

Usługi będą świadczone na zasadach analogicznych jak usługi świadczone w ramach świadczenia zamówienia podstawowego.

Oświadczenie o skorzystaniu z prawa opcji zostanie złożone przez Zamawiającego najpóźniej w 57 miesiącu świadczenia usług Wykonawcy.

Provisional timetable for recourse to these options:
in months: 60 (from the award of the contract)

II.2.3. Information about renewals

This contract is subject to renewal: no

II.3. Duration of the contract or time limit for completion

Duration in months: 60 (from the award of the contract)

Section III: Legal, economic, financial and technical information

III.1. Conditions related to the contract

III.1.1. Deposits and guarantees required

1. Wykonawcy zaproszeni do składania ofert będą zobowiązani do wniesienia wadium w wysokości: 6 000 000,00 zł (sześć milionów złotych).
2. Zabezpieczenie należytego wykonania umowy. Wyłoniony w postępowaniu Wykonawca, przed podpisaniem umowy zobowiązany będzie do wniesienia zabezpieczenia należytego wykonania umowy w wysokości 5 % ceny oferty brutto.

III.1.2. Main financing conditions and payment arrangements and/or reference to the relevant provisions governing them

Szczegółowe warunki finansowe zostaną określone w SWZ, która zostanie przekazana Wykonawcom zaproszonym do składania ofert. Wszystkie rozliczenia związane z realizacją niniejszego zamówienia publicznego dokonywane w złotych polskich (PLN).

III.1.3. Legal form to be taken by the group of economic operators to whom the contract is to be awarded

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia Wykonawcy powinni ustanowić pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy w sprawie niniejszego zamówienia zgodnie z art. 58 ustawy Pzp. Przed zawarciem umowy w sprawie zamówienia publicznego Zamawiający może żądać umowy regulującej współpracę tych Wykonawców.

III.1.4. Other particular conditions to which the performance of the contract is subject, in particular with regard to security of supply and security of information

1. O udzielenie zamówienia mogą ubiegać się wyłącznie Wykonawcy, którzy mają siedzibę albo miejsce zamieszkania w jednym z państw członkowskich Unii Europejskiej, Europejskiego Obszaru Gospodarczego lub państwie, z którym Unia Europejska lub Rzeczypospolita Polska zawarła umowę międzynarodową dotyczącą zamówień w dziedzinie obronności i bezpieczeństwa.
2. Wykonanie zamówienia wiąże się z przetwarzaniem informacji niejawnych o klauzuli tajności „poufne”. Na Wykonawcy ciąży obowiązek zapewnienia ochrony informacji niejawnych uzyskanych w trakcie postępowania o udzielenie zamówienia oraz po jego zakończeniu, w sposób określony w przepisach o ochronie informacji niejawnych.
3. Udział Wykonawców w Postępowaniu będzie wymagał zapoznania się z informacjami o klauzuli „zastrzeżone”, natomiast realizacja zamówienia będzie wymagała zapoznania się z informacjami o klauzuli „zastrzeżone” oraz „poufne”. W związku z powyższym Zamawiający

będzie weryfikował zdolność Wykonawcy do ochrony informacji niejawnych o klauzuli tajności minimum „poufne”, zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2023 r. poz. 756 z późn. zm.).

4. Zamawiający na etapie wniosku o dopuszczenie do udziału w postępowaniu będzie wymagał wykazania ww. zdolności od Wykonawcy, w tym każdego z Wykonawców wspólnie ubiegających się o zamówienie oraz podmiotów trzecich będących podwykonawcami Wykonawcy oraz wykazania, iż podmioty te posiadają akredytowane stanowiska komputerowe przeznaczone do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” lub wyżej. Szczegółowe wymagania w zakresie zapewnienia przez Wykonawcę bezpieczeństwa informacji niejawnych określone będą w Instrukcji Bezpieczeństwa Przemysłowego, która zostanie przekazana Wykonawcom zaproszonym do składania ofert wraz z SWZ.

5. Na drugim etapie postępowania Zamawiający będzie wymagał złożenia wraz z ofertą:

- 1) poświadczoną za zgodność z oryginałem kopii świadectwa bezpieczeństwa przemysłowego drugiego stopnia, potwierdzającej zdolność Wykonawcy/Wykonawców występujących wspólnie i znanych na tym etapie podwykonawców (przez które Zamawiający rozumie także podmioty udostępniające zasoby) do ochrony informacji niejawnych o klauzuli co najmniej „poufne”, wydanego przez ABW albo SKW (kopia świadectwa bezpieczeństwa przemysłowego poświadczona za „zgodność z oryginałem” przez osobę uprawnioną do reprezentowania Wykonawcy lub podwykonawcy, poświadczenie za zgodność winno być sporządzone w sposób umożliwiający identyfikację podpisu);
- 2) wykazu pracowników wyznaczonych do realizacji umowy, którzy w trakcie realizacji przedmiotowej umowy mogą mieć dostęp do informacji niejawnych, w tym także osoby uprawnionej do podpisania umowy oraz Pełnomocnika OIN Wykonawcy;
- 3) poświadczonych za zgodność z oryginałem kopii poświadczeń bezpieczeństwa i aktualnych zaświadczeń o odbytych szkoleniach w zakresie ochrony informacji niejawnych wszystkich osób wymienionych w wykazie, o którym mowa w ppkt 2) (kopie poświadczeń bezpieczeństwa i aktualnych zaświadczeń o odbytych szkoleniach w zakresie ochrony informacji niejawnych poświadczonych za „zgodność z oryginałem” przez osobę uprawnioną do reprezentowania Wykonawcy, poświadczenie za zgodność winno być sporządzone w sposób umożliwiający identyfikację podpisu);
- 4) oświadczenia Wykonawcy o zobowiązaniu wszystkich pracowników i podwykonawców do ochrony informacji niejawnych, które pozyskają w trakcie Postępowania lub w trakcie realizacji zamówienia.

III.1.5. Information about security clearance

III.2. Conditions for participation

III.2.1. Personal situation

Criteria regarding the personal situation of economic operators (that may lead to their exclusion) including requirements relating to enrolment on professional or trade registers

List and brief description of conditions: I. Podstawy wykluczenia

O udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 108 ust. 1 i ust. 2, art. 405 ust. 2 pkt 1, 2, 3, 4, 6, 7 oraz art. 405 ust. 2 pkt 5 w zakresie art. 109 ust. 1 pkt 1 i 4 ustawy Pzp.

Z postępowania o udzielenie zamówienia wyklucza się Wykonawcę:

1. będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
 - b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
 - c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego, w art. 46–48 ustawy z dnia 25

czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1-4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2022r. poz. 463, 583 i 9744),

d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,

e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. 2021 poz. 1745),

g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,

h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

– lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2. jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;

3. wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

4. wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

5. jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów złożyli odrębne wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te wnioski niezależnie od siebie;

6. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 ustawy, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia;

7. który udaremnia lub utrudnia stwierdzenie przestępnego pochodzenia pieniędzy lub ukrywa ich pochodzenie, w związku z brakiem możliwości ustalenia beneficjenta rzeczywistego, w rozumieniu art. 2 ust. 2 pkt 1 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2020 r. poz. 971, 875, 1086 i 2320 oraz z

2021 r. poz. 187 i 815).

8. Zamawiający wykluczy również Wykonawcę:

1) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3 ustawy Pzp, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

2) w stosunku do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury;

3) będącego osobą fizyczną, spółką jawną, spółką partnerską, spółką komandytową, spółką komandytowo-akcyjną albo osobą prawną, jeżeli, odpowiednio, w stosunku do takiej osoby, wspólnika, partnera lub członka zarządu, komplementariusza, urzędującego członka organu zarządzającego, lub w związku z podejmowanym przez niego działaniem lub zaniechaniem podjęto decyzję o cofnięciu poświadczenia bezpieczeństwa, o której mowa w art. 33 ust. 11 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

4) który naruszył zobowiązania w zakresie bezpieczeństwa informacji lub bezpieczeństwa dostaw;

5) którego uznano za nieposiadającego wiarygodności niezbędnej do wykluczenia zagrożenia dla obronności lub bezpieczeństwa państwa, także w inny sposób niż w drodze wydania decyzji o cofnięciu świadectwa bezpieczeństwa przemysłowego, o której mowa w art. 66 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;

6) który ma siedzibę albo miejsce zamieszkania w innym państwie niż państwa, o których mowa w art. 404 ust. 1, z zastrzeżeniem art. 404 ust. 2;

7) będącego osobą fizyczną, która naruszyła zobowiązania dotyczące bezpieczeństwa informacji lub bezpieczeństwa dostaw, w związku z wykonaniem, niewykonaniem lub nienależytym wykonaniem zamówienia;

8) jeżeli urzędujący członek jego organu zarządzającego lub nadzorczego, wspólnik spółki w spółce jawnej lub partnerskiej albo komplementariusz w spółce komandytowej lub komandytowo-akcyjnej lub prokurent naruszył zobowiązania dotyczące bezpieczeństwa informacji lub bezpieczeństwa dostaw w związku z wykonaniem, niewykonaniem lub nienależytym wykonaniem zamówienia

9. O udzielenie zamówienia mogą się ubiegać Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 7 ust 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego oraz na podstawie art. 5k Rozporządzenia Rady (UE) nr 2022 /576 z dnia 8 kwietnia 2022 r. w sprawie zmiany Rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str.1).

Criteria regarding the personal situation of subcontractors (that may lead to their rejection) including requirements relating to enrolment on professional or trade registers

List and brief description of conditions: Wykaz oświadczeń lub dokumentów tj. podmiotowych środków dowodowych potwierdzających brak podstaw wykluczenia z postępowania.

I. Wykonawca zobowiązany jest złożyć wraz z Wnioskiem o dopuszczenie do udziału w postępowaniu:

1. informację z Krajowego Rejestru Karnego w zakresie: art. 108 ust. 1 pkt 1 i 2 ustawy Pzp, art. 108 ust. 1 pkt 4 ustawy Pzp dotyczącej orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka karnego – wystawioną nie wcześniej niż 6 miesięcy przed upływem

- terminu składania wniosków o dopuszczenie do udziału w postępowaniu;
2. oświadczenie Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie wniosku o dopuszczenie do udziału w postępowaniu niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej, sporządzonego zgodnie z Załącznikiem nr 7 do Wniosku o dopuszczenie do udziału w postępowaniu;
3. zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzającego, że Wykonawca nie zalega z opłacaniem podatków i opłat, w zakresie art. 109 ust. 1 pkt 1 ustawy Pzp, wystawione nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem podatków lub opłat wraz z zaświadczeniem Zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu Wykonawca dokonał płatności należnych podatków lub opłat wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
4. zaświadczenie albo inny dokument właściwej terenowej jednostki organizacyjnej Zakładu Ubezpieczeń Społecznych lub właściwego oddziału regionalnego lub właściwej placówki terenowej Kasy Rolniczego Ubezpieczenia Społecznego potwierdzającego, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne i zdrowotne, w zakresie art. 109 ust. 1 pkt 1 ustawy Pzp, wystawionego nie wcześniej niż 3 miesiące przed jego złożeniem, a w przypadku zalegania z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne wraz z zaświadczeniem albo innym dokumentem Zamawiający żąda złożenia dokumentów potwierdzających, że odpowiednio przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu Wykonawca dokonał płatności należnych składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłat tych należności;
5. odpis lub informację z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy Pzp, sporządzoną nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
6. informację z Centralnego Rejestru Beneficjentów Rzeczywistych, w zakresie art. 108 ust. 2 ustawy Pzp, jeżeli odrębne przepisy wymagają wpisu do tego rejestru, sporządzoną nie wcześniej niż 3 miesiące przed jej złożeniem;
7. oświadczenie o niepodleganiu wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego oraz na podstawie art. 5 k Rozporządzenia Rady (UE) nr 833/2014 z dnia 31 lipca 2014 r. dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 229 z 31.7.2014, str. 1) dodanego Rozporządzeniem Rady (UE) nr 2022/576 z dnia 8 kwietnia 2022 r. w sprawie zmiany rozporządzenia (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie (Dz. Urz. UE nr L 111 z 8.4.2022, str.1), zgodnie z Załącznikiem nr 5 do Wniosku o dopuszczenie do udziału w postępowaniu (w przypadku Wykonawcy/Wykonawców ubiegających się wspólnie o zamówienie) lub z Załącznikiem nr 6 do Wniosku o dopuszczenie do udziału w postępowaniu (w przypadku podmiotów trzecich udostępniających potencjał);
8. oświadczenie o braku podstaw wykluczenia wymienionych w z postępowania wskazanych przez zamawiającego, o których mowa w:
- a) art. 108 ust. 1 pkt 3 ustawy Pzp,

- b) art. 108 ust. 1 pkt 4 ustawy Pzp, dotyczących orzeczenia zakazu ubiegania się o zamówienie publiczne tytułem środka zapobiegawczego,
- c) art. 108 ust. 1 pkt 5 ustawy Pzp, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
- d) art. 108 ust. 1 pkt 6 ustawy Pzp,
- e) art. 109 ust. 1 pkt 1 ustawy Pzp, odnośnie do naruszenia obowiązków dotyczących płatności podatków i opłat lokalnych, o których mowa w ustawie z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych (Dz.U. z 2019 r. poz. 1170), zgodnie z załącznikiem nr 10 do Wniosku o dopuszczenie do udziału w postępowaniu.
9. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, należy wraz z wnioskiem złożyć dokumenty wskazane w pkt 1 - 8 dotyczące każdego z Wykonawców wspólnie ubiegających się o udzielenie zamówienia, w celu wykazania braku istnienia wobec niego podstaw wykluczenia;
10. Jeżeli Wykonawca polega na zasobach podmiotu trzeciego/podmiotów trzecich, należy wraz z wnioskiem złożyć dokumenty dotyczące podmiotu trzeciego/podmiotów trzecich, na których zdolnościach technicznych polega Wykonawca, w celu wykazania braku istnienia wobec nich podstaw wykluczenia, wymienione w pkt 1, 3, 4, 5, 7 i 8.
- II. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast:
1. informacji z Krajowego Rejestru Karnego, o której mowa pkt 1. powyżej – składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie, o którym mowa w pkt 1 powyżej. Dokument powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu;
 2. informacji z Centralnego Rejestru Beneficjentów Rzeczywistych, o której mowa w pkt 6. powyżej – składa informację z odpowiedniego rejestru zawierającego informacje o jego beneficjentach rzeczywistych albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, określający jego beneficjentów rzeczywistych wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu;
 3. zaświadczenia, o którym mowa w pkt 3. powyżej zaświadczenia albo innego dokumentu potwierdzającego, że wykonawca nie zalega z opłacaniem składek na ubezpieczenia społeczne lub zdrowotne, o których mowa w pkt 4 powyżej, lub odpisu albo informacji z Krajowego Rejestru Sądowego lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, o których mowa w pkt 5 powyżej – składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:
 - a) nie naruszył obowiązków dotyczących płatności podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne,
 - b) nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury.Dokument, o którym mowa w pkt 1, powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu. Dokumenty, o których mowa w pkt 2 i 3 powinny być wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu.

4. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy dokument, nie wydaje się dokumentów, o których mowa w pkt 1 lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4, art. 109 ust. 1 pkt 1 ustawy Pzp, zastępuje się je odpowiednio w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy lub miejsce zamieszkania ma osoba, której dokument miał dotyczyć. W takim przypadku, dokumenty te powinny być wystawione odpowiednio nie wcześniej niż 6 lub 3 miesiące przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu, zgodnie z zasadami określonymi w pkt 1) lub pkt 3).

III.2.2. Economic and financial ability

Criteria regarding the economic and financial standing of economic operators (that may lead to their exclusion)

List and brief description of conditions: Zamawiający nie precyzuje warunków w tym zakresie.
Minimum level(s) of standards possibly required: Zamawiający nie precyzuje warunków w tym zakresie.

Criteria regarding the economic and financial standing of subcontractors (that may lead to their rejection)

List and brief description of conditions: Zamawiający nie precyzuje warunków w tym zakresie.
Minimum level(s) of standards possibly required: Zamawiający nie precyzuje warunków w tym zakresie.

III.2.3. Technical and/or professional capacity

Criteria regarding the technical and/or professional ability of economic operators (that may lead to their exclusion)

List and brief description of conditions:

WARUNKI UDZIAŁU W POSTĘPOWANIU

O udzielenie zamówienia ubiegać się mogą Wykonawcy, którzy spełniają następujące warunki dotyczące:

1) zdolności technicznej lub zawodowej:

A. Wykonawca spełni warunek, jeżeli wykaże, że:

- posiada zdolność do ochrony informacji niejawnych i ich przetwarzania o klauzuli tajności minimum „poufne” zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz.U. z 2023 r. poz. 756 z późn. zm.).

– posiada akredytowane stanowiska komputerowe przeznaczone do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”,

B. Wykonawca spełni warunek, jeżeli wykaże, że w okresie ostatnich 5 (pięciu) lat przed upływem terminu składania wniosków o dopuszczenie do udziału w Postępowaniu:

1) przez okres minimum 2 lat należycie utrzymywał lub utrzymuje system DLP - Data Loss Prevention obejmujący co najmniej 20 000 licencji;

2) przez okres minimum 2 lat należycie utrzymywał lub utrzymuje system PAM - Privileged Access Management obejmujący co najmniej 450 licencji;

3) przez okres minimum 2 lat należycie utrzymywał lub utrzymuje system ETD - Enterprise Threat Detection obejmujący co najmniej 20 000 licencji;

- 4) przez okres minimum 2 lat należycie utrzymywał lub utrzymuje system Anty ATP - Anty Advanced Threat Protection obejmujący co najmniej 20 000 licencji;
- 5) przez okres minimum 2 lat należycie utrzymywał lub utrzymuje system zapewniający bezpieczeństwo w zakresie rozszyfrowywania ruchu sieciowego ochrony stacji roboczych (oprogramowanie antywirusowe) obejmujący co najmniej 25 000 licencji;
- 6) przez okres minimum 2 lat należycie utrzymywał lub utrzymuje system SIEM - Security Information and Event Management;
- 7) przez okres minimum 2 lat należycie utrzymywał lub utrzymuje co najmniej jeden z systemów: DAM – Database Activity Monitoring, SOAR – Security Orchestration, Automation and Respons, WAF – Web Application Firewall.

C. Wykonawca spełni warunek, jeżeli wykaże, że w okresie ostatnich 5 (pięciu) lat przed upływem terminu składania wniosków o dopuszczenie do udziału w Postępowaniu przez okres minimum 2 lat należycie świadczył na rzecz klienta Wykonawcy (odrębny podmiot) usługi odnoszące się do systemu obejmującego min. 20 000 licencji (dalej jako „System”) polegające co najmniej na:

- ocenie oprogramowania/produktów przygotowanych przez innego wykonawcę (odrębny podmiot) dla klienta Wykonawcy, w tym wykonywanie testów regresji, międzymodułowych, wydajnościowych i bezpieczeństwa oprogramowania stworzonego przez innego wykonawcę,
- doradzaniu w zakresie rozwoju lub modyfikacji Systemu w tym ocenie wpływu rozwoju (nowych rozwiązań) na Infrastrukturę techniczno–systemową klienta.

W przypadku wykazywania warunków określonych w lit B pkt 1-5 Zamawiający wymaga, aby do upływu terminu składania wniosków o udzielenie zamówienia okres należycie świadczonych przez Wykonawcę usług trwał przez co najmniej 2 lata w trakcie 5 lat licząc od dnia składania wniosku o dopuszczenie do udziału w postępowaniu.

Ponadto, wykazywane doświadczenie Wykonawcy będzie weryfikowane z uwzględnieniem następujących reguł:

- 1) okres doświadczenia zdobytego w ramach utrzymania różnych systemów, realizowanych w tym samym czasie - nie podlega sumowaniu,
- 2) doświadczenie zdobyte w zakresie utrzymania systemów w różnym czasie podlega sumowaniu, z tym, że w przypadku, gdy Wykonawca wykaże utrzymanie systemów, których okresy realizacji zachodzą na siebie, będą one liczone jednokrotnie, tj. Zamawiający do okresu doświadczenia zaliczy okres od dnia rozpoczęcia wcześniejszego utrzymania systemu do dnia zakończenia późniejszego utrzymania systemu,
- 3) w przypadku braku podania daty dziennej a jedynie informacji o miesiącu, Zamawiający na potrzeby ustalenia okresu doświadczenia przyjmie ostatni dzień danego miesiąca (dla rozpoczęcia utrzymania systemu) oraz pierwszy dzień danego miesiąca (dla zakończenia utrzymania systemu),
- 4) w przypadku podania jedynie informacji o roku rozpoczęcia lub zakończenia utrzymania systemu, Zamawiający na potrzeby ustalenia okresu doświadczenia, przyjmie 31 grudnia danego roku (dla rozpoczęcia utrzymania systemu) oraz 1 stycznia danego roku (dla zakończenia utrzymania systemu).

UWAGA nr 1:

W odniesieniu do warunków dotyczących zdolności technicznej lub zawodowej w zakresie doświadczenia Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z Wykonawców, którzy wykonają usługi, do realizacji których te zdolności są wymagane.

UWAGA nr 2:

Zamawiający wymaga, aby każdy z Wykonawców wspólnie ubiegających się o zamówienie lub podmiot trzeci użyzający potencjał doświadczenia spełniał warunek określony w lit. A (tj. posiadał zdolność do ochrony informacji niejawnych i ich przetwarzania o klauzuli tajności

minimum „poufne” oraz akredytowane stanowiska komputerowe przeznaczone do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”).

Zamawiający dopuszcza wykazanie spełnienia warunków udziału w postępowaniu, o których mowa w pkt B, odrębnie dla warunków określonych w pkt 1-7. Oznacza to, że możliwe jest sumowanie doświadczenia w ramach warunku dot. zdolności technicznej lub zawodowej w ten sposób, że jeden Wykonawca /podmiot trzeci wykaże się jedną, kilkoma lub wszystkimi usługami wskazanymi w lit. B od 1 do 7 z zastrzeżeniem, że każdorazowo Wykonawca ten lub podmiot trzeci musi jednocześnie wykazać spełnienie warunku określonego w lit. A. Nie dopuszcza się sumowania doświadczenia w ramach jednego warunku np. kilku mniejszych systemów DLP w celu wykazania spełniania warunku określonego w lit. B pkt 1.

Przez „usługę” należy rozumieć usługę świadczoną na rzecz tego samego zamawiającego /klienta, co oznacza, że dopuszczalne jest sumowanie okresów doświadczenia w ramach różnych umów u jednego zamawiającego/klienta).

UWAGA nr 3:

Wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają do wniosku o dopuszczenie do udziału w postępowaniu oświadczenie, z którego wynika, które usługi wykonają poszczególni Wykonawcy (zgodnie z Załącznikiem nr 4 do Wniosku o dopuszczenie do udziału w postępowaniu).

UWAGA nr 4:

Nie dopuszcza się użyczenia potencjału w zakresie, w jakim Zamawiający żąda samodzielnego świadczenia usług Integratora Bezpieczeństwa tj. warunku wskazanego w lit C oraz osób nazywanych Integratorami bezpieczeństwa określonych w lit D.

D. Wykonawca spełni warunek, jeżeli wykaże, że dysponuje lub będzie dysponować osobami skierowanymi przez Wykonawcę do realizacji zamówienia (tj. skierowanymi do realizacji umowy), o odpowiednich kwalifikacjach zawodowych, uprawnieniach, doświadczeniu i wykształceniu, odpowiednimi do funkcji, jakie zostaną im powierzone, tj.:

1) minimum 1 (jedną) osobą do pełnienia funkcji Kierownika projektu w zakresie usług dodatkowych, które powinny się cechować następującymi kompetencjami:

a) posiada minimum 5-letnie doświadczenie zawodowe rozumiane jako udział w realizacji projektów informatycznych,

b) posiada co najmniej 36 miesięcy doświadczenia zawodowego w zakresie pełnienia funkcji kierownika lub zastępcy kierownika w projekcie /projektach informatycznych o wartości minimum 3 000 000,00 PLN brutto każdy projekt, dotyczących bezpieczeństwa, polegających na budowie lub rozwoju systemu informatycznego/systemów informatycznych, uzyskanego w ciągu ostatnich 5 lat przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu;

c) posiada certyfikat PRINCE2 Practitioner lub równoważny dokument/certyfikat wystawiony przez podmiot niezależny od Wykonawcy;

d) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o którym mowa w ustawie o ochronie informacji niejawnych;

e) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;

2) minimum 3 (trzema) osobami do pełnienia funkcji Specjalistów ds. cyberbezpieczeństwa (Integrator Bezpieczeństwa), które powinny się cechować następującymi kompetencjami:

a) posiada co najmniej 36 miesięcy doświadczenia zawodowego w realizacji prac związanych z instalowaniem i serwisowaniem urządzeń i systemów bezpieczeństwa w projekcie /projektach informatycznych o wartości minimum 5 000 000 PLN brutto każdy projekt, polegających na budowie lub rozwoju systemów informatycznych, uzyskanego w ciągu ostatnich 5 lat przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu;

b) posiada co najmniej dwa z niżej wymienionych certyfikatów:

- Certified Information Systems Auditor (CISA),
- Certified Information Security Manager (CISM),
- ISACA's Certified in Risk and Information Systems Control (CRISC),
- Certified Information Systems Security Professional (CISSP),
- Certified Ethical Hacker (CEH),
- Offensive Security Certified Professional – (OSCP);

lub równoważnych certyfikatów wystawionych przez podmiot niezależny od Wykonawcy;

c) posiada umiejętności zakończone pozytywnym wynikiem egzaminu poświadczającym możliwość realizowania audytów jako audytor wiodący ISO27001;

d) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o których którym mowa w ustawie o ochronie informacji niejawnych;

e) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;

3) minimum 2 (dwoma) osobami do pełnienia funkcji Konsultanta wdrożeń bezpośrednich, które powinny się cechować następującymi kompetencjami:

a) posiada minimum 3-letnie doświadczenie zawodowe w branży IT,

b) posiada co najmniej 24 miesięczne doświadczenie zawodowe, uzyskane w ciągu ostatnich 5 lat przed terminem składania wniosków o dopuszczenie do udziału w postępowaniu, we wdrażaniu oprogramowania systemów bezpieczeństwa;

4) minimum 1 (jedną) osobą do pełnienia funkcji Analityka biznesowego, która powinna się cechować następującymi kompetencjami:

a) posiada minimum 5-letnie doświadczenie zawodowe w branży IT,

b) pełniła rolę Analityka procesów biznesowych / Analityka biznesowego w minimum 1 projekcie IT związanym z analizą i dostosowaniem procesów biznesowych w zakresie bezpieczeństwa;

c) posiada co najmniej 24-miesięczne doświadczenie zawodowe, uzyskane w ciągu ostatnich 5 lat przed terminem składania wniosków o dopuszczenie do udziału w postępowaniu, w modelowaniu procesów biznesowych w zakresie bezpieczeństwa;

d) posiada znajomość:

- przepisów ustawy o: Krajowym systemie Cyberbezpieczeństwa (KSC); Informatyzacji działalności podmiotów realizujących zadania publiczne,
- przepisów rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;

5) minimum 3 (trzema) osobami do pełnienia funkcji Testerów bezpieczeństwa, które powinny się cechować następującymi kompetencjami:

a) w ciągu ostatnich 36 miesięcy przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu, tworzyła plany testów i scenariuszy testowych oraz przeprowadzała testy poniższymi metodykami:

- Blackbox,
- Whitebox,
- Greybox;

b) posiada certyfikat Certified Ethical Hacker (CEH) lub równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;

c) posiada co najmniej jeden z niżej wymienionych certyfikatów:

- Offensive Security Wireless Professional (OSWP)
- Offensive Security Certified Expert (OSCE),
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) ,
- eLearnSecurity Web application Penetration Tester (eWPT),

- eLearnSecurity Web application Penetration Tester eXtreme (eWPTX),
 - eLearnSecurity Mobile Application Penetration Tester (eMAPT)
- lub równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;
- d) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o których którym mowa w ustawie o ochronie informacji niejawnych;
- e) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;
- 6) minimum 1 (jedną) osobą zajmująca się wydajnością systemu (Integrator Bezpieczeństwa), która powinna się cechować następującymi kompetencjami:
- a) w ciągu ostatnich 36 miesięcy przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu, uczestniczyła w minimum 2 projektach informatycznych, w których zajmowała się optymalizacją wydajności systemów informatycznych;
 - b) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o których którym mowa w ustawie o ochronie informacji niejawnych;
 - c) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;
- 7) minimum 1 (jedną) osobę do pełnienia funkcji Specjalisty ds. konfigurowania i utrzymania środowisk nieprodukcyjnych (Integrator Bezpieczeństwa), która powinna się cechować następującymi kompetencjami:
- a) posiada minimum 5-letnie doświadczenie zawodowe w branży IT,
 - b) posiada co najmniej 24-miesięczne doświadczenie zawodowe, uzyskane w ciągu ostatnich 5 lat przed terminem składania wniosków o dopuszczenie do udziału w postępowaniu, polegające na uczestniczeniu w konfigurowaniu i utrzymaniu środowisk do testów oprogramowania i usług;
- 8) minimum 1 (jedną) osobą do pełnienia funkcji Eksperta walidacji i testów usług (Integrator Bezpieczeństwa), która powinna się cechować następującymi kompetencjami:
- a) posiada minimum 5-letnie doświadczenie zawodowe w branży IT,
 - b) posiada co najmniej 24-miesięczne doświadczenie zawodowe uzyskane w ciągu ostatnich 5 lat przed terminem składania wniosków o dopuszczenie do udziału w postępowaniu, w ramach usług utrzymania systemu informatycznego, w realizowaniu prac związanych z testowaniem oprogramowania lub usług IT oraz utrzymaniem środowiska testowego;
 - c) posiada znajomość metodyk testowania oprogramowania;
 - d) posiada certyfikat ITIL Release lub Control Validation lub ISTQB Certified Tester, lub równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;
- 9) minimum 1 (jedną) osobą, do pełnienia funkcji Architekta bezpieczeństwa (Integrator Bezpieczeństwa), która powinna się cechować następującymi kompetencjami:
- a) posiada minimum 3-letnie doświadczenie zawodowe uzyskane w ciągu ostatnich 5 lat przed terminem składania wniosków o dopuszczenie do udziału w postępowaniu, rozumiane jako udział w realizacji projektów informatycznych polegających na budowie lub rozwoju systemów bezpieczeństwa, jako architekt bezpieczeństwa;
 - b) w ciągu ostatnich 5 lat przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu brała udział jako architekt bezpieczeństwa w co najmniej 2 projektach polegających na zaprojektowaniu systemu bezpieczeństwa dla systemu o następujących cechach:
 - zorientowany na usługi,
 - w architekturze wielowarstwowej,
 - o wysokiej wydajności i niezawodności,
 - wykorzystujący bazy danych;
 - c) posiada umiejętności tworzenia dokumentacji analitycznej przy wykorzystaniu narzędzia CASE i notacji UML;

- d) posiada certyfikat CISSP (Certified Information Systems Security Professional) lub równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;
- e) posiada umiejętności zakończone pozytywnym wynikiem egzaminu poświadczającym możliwość realizowania audytów jako audytor wiodący ISO27001;
- f) posiada ważne poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli tajności „poufne”, o których mowa w ustawie o ochronie informacji niejawnych;
- g) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;
- 10) minimum 2 (dwoma) osobami do pełnienia funkcji Administratora DLP, z których każda powinna cechować następującymi kompetencjami:
- a) w ciągu ostatnich 36 miesięcy przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu, przez okres co najmniej 2 lat administrowała systemem DLP – Data Loss Prevention i posiada certyfikat producenta systemu DLP potwierdzający jej kompetencje administratorskie;
- b) posiada co najmniej jeden z poniższych certyfikatów:
- Certified Information Systems Auditor (CISA),
 - Security+ (CompTIA Security+);
- lub inny równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;
- c) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o którym mowa w ustawie o ochronie informacji niejawnych;
- d) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;
- 11) minimum 2 (dwoma) osobami do pełnienia funkcji Administratora PAM, z których każda powinna cechować następującymi kompetencjami:
- a) w ciągu ostatnich 36 miesięcy przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu, przez okres co najmniej 2 lat administrowała systemem PAM – Privileged Access Management i posiada co najmniej jeden certyfikat producenta rozwiązań PAM potwierdzający jej kompetencje administratorskie;
- b) posiada co najmniej jeden z poniższych certyfikatów:
- Certified Information Systems Auditor (CISA),
 - Security+ (CompTIA Security+);
- lub inny równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;
- c) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o którym mowa w ustawie o ochronie informacji niejawnych;
- d) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;
- 12) minimum 2 (dwoma) osobami do pełnienia funkcji Administratora ETD, z których każda powinna się cechować następującymi kompetencjami:
- a) w ciągu ostatnich 36 miesięcy przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu, przez okres co najmniej 2 lat administrowała systemem ETD – Enterprise Threat Detection i posiada co najmniej jeden certyfikat producenta rozwiązań ETD potwierdzający jej kompetencje administratorskie;
- b) posiada co najmniej jeden z poniższych certyfikatów:
- Certified Information Systems Auditor (CISA),
 - Security+ (CompTIA Security+)
- lub inny równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;
- c) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o którym mowa w ustawie o ochronie informacji niejawnych;
- d) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji

niejawnych;

13) minimum 2 (dwoma) osobami do pełnienia funkcji Administratora Anty ATP, z których każda powinna się cechować następującymi kompetencjami:

a) w ciągu ostatnich 36 miesięcy przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu, przez okres co najmniej 2 lat administrowała systemem Anty ATP - Anty Advanced Threat Protection i posiada co najmniej jeden certyfikat producenta rozwiązań Anty ATP potwierdzający jej kompetencje administratorskie;

b) posiada co najmniej jeden z poniższych certyfikatów:

- Certified Information Systems Auditor (CISA),
- Cerified Ethical Hacker (CEH);
- Security+ (CompTIA Security+)

lub inny równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;

c) posiada ważne upoważnienie uprawniające do dostępu do informacji niejawnych o klauzuli tajności „zastrzeżone”, o którym mowa w ustawie o ochronie informacji;

d) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych;

14) 1 (jedną) osobą do pełnienia funkcji Dyrektora Umowy, która powinna się cechować następującymi kompetencjami:

a) posiada minimum 5-letnie doświadczenie zawodowe w branży IT związane z prowadzeniem projektów,

b) w ciągu ostatnich 5 lat przed dniem składania wniosków o dopuszczenie do udziału w postępowaniu, pełniła rolę Kierownika projektu IT w 2 projektach przez co najmniej 6 miesięcy każdy, o łącznej wartości nie niższej niż 20 000 000 zł brutto;

c) posiada certyfikat PRINCE2 Practitioner lub PMP lub IPMA Level A, lub inny równoważny certyfikat wystawiony przez podmiot niezależny od Wykonawcy;

d) posiada ważne poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli tajności „poufne”, o których mowa w ustawie o ochronie informacji niejawnych;

e) posiada zaświadczenie stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych.

Zamawiający dopuszcza wskazanie jednej osoby do pełnienia nie więcej niż dwóch funkcji spośród wymienionych powyżej w pkt 10), 11), 12), 13). Łączenie funkcji jest możliwe wyłącznie w zakresie funkcji administratorów systemów (nie więcej niż dwóch). W pozostałym zakresie Zamawiający nie dopuszcza wykazywania warunków dla różnych funkcji przez jedną osobę.

DEFINICJE:

bezpieczeństwo – pod tym pojęciem Zamawiający rozumie zagadnienia w obszarze bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa;

systemy bezpieczeństwa – pod tym pojęciem Zamawiający rozumie wszelkie systemy służące do zapewnienia wysokiego poziomu bezpieczeństwa informacji.

Zamawiający informuje, że doświadczenie zawodowe osób wskazanych na potwierdzenie spełnienia warunku, o którym mowa w lit. D w realizacji wykazywanych zadań / projektów, będzie liczone w następujący sposób:

1) okres doświadczenia zawodowego zdobytego w ramach różnych zadań / projektów , w których brała udział dana osoba i realizowanych w tym samym czasie - nie podlega sumowaniu,

2) doświadczenie zawodowe zdobyte w zakresie wykazanych zadań / projektów, w których brała udział dana osoba, w różnym czasie podlega sumowaniu, z tym, że w przypadku, gdy Wykonawca wykaże zadania / projekty, których okresy realizacji zachodzą na siebie, będą one liczone jednokrotnie, tj. Zamawiający do doświadczenia zawodowego uzna okres od dnia

rozpoczęcia wcześniejszego zadania / projektu do dnia zakończenia późniejszego zadania / projektu,

3) wartość projektu określona będzie jako wartość projektu wynikająca z umowy, a w przypadku projektów realizowanych na podstawie kilku umów – wartość wynikająca z tych umów,

4) w przypadku braku podania daty dziennej, a jedynie informacji o miesiącu, Zamawiający na potrzeby ustalenia okresu doświadczenia zawodowego przyjmie ostatni dzień danego miesiąca (dla rozpoczęcia zadania / projektu) oraz pierwszy dzień danego miesiąca (dla zakończenia zadania / projektu),

5) w przypadku podania jedynie informacji o roku rozpoczęcia lub zakończenia zadania / projektu, Zamawiający na potrzeby ustalenia okresu doświadczenia zawodowego przyjmie 31 grudnia danego roku (dla rozpoczęcia zadania / projektu) oraz 1 stycznia danego roku (dla zakończenia zadania / projektu).

Oceniając zdolność techniczną lub zawodową, Zamawiający może, na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez Wykonawcę sprzecznych interesów, w szczególności zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy, może mieć negatywny wpływ na realizację zamówienia.

UWAGA nr 1:

Zamawiający zastrzega obowiązek osobistego wykonania przez Wykonawcę kluczowych zadań dotyczących świadczenia usługi w zakresie Integratora Bezpieczeństwa.

Zakres zadań dla Integratora Bezpieczeństwa jest zastrzeżony do osobistego wykonania przez Wykonawcę, a zatem Wykonawca musi samodzielnie spełniać warunki udziału w postępowaniu dla Integratora Bezpieczeństwa tj. warunku doświadczenia wskazanego w lit C oraz dysponowania bezpośrednio osobami określonymi jako Integratorzy bezpieczeństwa w warunku wskazanym w lit. D. Nie dopuszcza się wykazywania tych warunków na podstawie zdolności podmiotów udostępniających zasoby oraz realizacji zamówienia w tym zakresie przy pomocy podwykonawców.

UWAGA nr 2:

Wykonawca nie może, po upływie terminu składania wniosków o dopuszczenie do udziału w postępowaniu, powoływać się na zdolności podmiotów udostępniających zasoby, jeżeli na etapie składania wniosków o dopuszczenie do udziału w postępowaniu nie polegał on w danym zakresie na zdolnościach podmiotów udostępniających zasoby.

Wykonawca, który polega na zdolnościach podmiotów udostępniających zasoby, składa, wraz z wnioskiem o dopuszczenie do udziału w postępowaniu, zobowiązanie podmiotu udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia (sporządzone zgodnie z Załącznikiem nr 3 do Wniosku o dopuszczenie do udziału w postępowaniu) lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów.

Zobowiązanie podmiotu udostępniającego zasoby lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, ma potwierdzać, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określać, w szczególności:

- zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
- sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
- czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach, którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia,

kwalifikacji zawodowych lub doświadczenia, zrealizuje usługi, których wskazane zdolności dotyczą.

Zamawiający oceni, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełniania warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.

Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełniania przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wykazał, że samodzielnie spełnia warunki udziału w postępowaniu.

Minimum level(s) of standards possibly required

Wraz z wnioskiem o dopuszczenie do udziału w postępowaniu Wykonawca zobowiązany jest złożyć:

1. Aktualne na dzień składania wniosków o dopuszczenie do udziału w postępowaniu oświadczenie o niepodleganiu wykluczeniu i spełnianiu warunków udziału w postępowaniu, o którym mowa w art. 125 ust. 1 ustawy Pzp (sporządzone zgodnie z Załącznikiem nr 2 do Wniosku o dopuszczenie do udziału w postępowaniu).

W przypadku wspólnego ubiegania się o udzielenie zamówienia przez Wykonawców ww. oświadczenie składa każdy z nich.

Wykonawca, w przypadku polegania na zdolnościach podmiotów udostępniających zasoby, przedstawia wraz z ww. oświadczeniem, także oświadczenie podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz spełnianie warunków udziału w postępowaniu, w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

2. Zobowiązanie podmiotu udostępniającego zasoby do oddania Wykonawcy do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tego podmiotu.

3. W przypadku, gdy Wykonawcę reprezentuje pełnomocnik – pełnomocnictwo określające jego zakres, podpisane przez osobę/y upoważnione do reprezentacji wskazane we właściwym rejestrze, z którego wynika prawo do podpisania Wniosku o dopuszczenie do udziału w postępowaniu oraz do podpisania innych dokumentów składanych wraz z wnioskiem o dopuszczenie do udziału w postępowaniu. W przypadku, gdy Wniosek o dopuszczenie do udziału w postępowaniu składają Wykonawcy ubiegający się wspólnie o udzielenie zamówienia, pełnomocnictwo określające zakres umocowania pełnomocnika ustanowionego do reprezentowania ich w postępowaniu.

4. Na potwierdzenie spełnienia warunków udziału w postępowaniu o udzielenie zamówienia:

1) w zakresie warunku wskazanego w lit A:

a) ważne świadectwo bezpieczeństwa przemysłowego co najmniej II stopnia, potwierdzające zdolność przedsiębiorcy (Wykonawcy/podmiotu trzeciego) do ochrony informacji niejawnych o klauzuli tajności co najmniej „poufne” wydane na podstawie ustawy o ochronie informacji niejawnych (z wyłączeniem możliwości ich przetwarzania we własnych systemach teleinformatycznych),

b) oświadczenie, że (Wykonawca/Wykonawcy lub podmiot trzeci posiada akredytowane stanowiska komputerowe przeznaczone do przetwarzania informacji niejawnych o klauzuli „zastrzeżone” – według wzoru stanowiącego Załącznik nr 11 do Wniosku o dopuszczenie do udziału w postępowaniu;

2) W zakresie warunków wskazanych w lit. B i C – wykaz usług wykonanych w okresie ostatnich 5 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których usługi

zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te usługi zostały wykonane lub są wykonywane należycie – według wzoru stanowiącego Załącznik nr 8 do Wniosku o dopuszczenie do udziału w postępowaniu;

Dowodami potwierdzającymi, czy usługi zostały wykonane należycie, są:

- referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych – są wykonywane, w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy,

- inne odpowiednie dokumenty – jeżeli Wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy,

3) w zakresie warunku wskazanego w lit. D – wykaz osób skierowanych przez Wykonawcę do realizacji zamówienia publicznego wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami – według wzoru stanowiącego Załącznik nr 9 do Wniosku o dopuszczenie do udziału w postępowaniu.

Criteria regarding the technical and/or professional ability of subcontractors (that may lead to their rejection)

III.2.4. Information about reserved contracts

III.3. Conditions specific to services contracts

III.3.1. Information about a particular profession

Execution of the service is reserved to a particular profession: no

III.3.2. Information about staff responsible for the performance of the contract

Obligation to indicate the names and professional qualifications of the staff assigned to performing the contract: yes

Section IV: Procedure

IV.1. Type of procedure

IV.1.1. Type of procedure

Restricted

IV.1.2. Information about the limits on the number of candidates to be invited

Envisaged minimum number 3

Objective criteria for choosing the limited number of candidates: 1. Ocena spełniania postawionych warunków dokonana zostanie zgodnie z formułą spełnia/nie spełnia, w oparciu o dokumenty wymagane zapisami sekcji III.2.1) i III.2.3) Ogłoszenia. Z treści załączonych dokumentów musi wynikać jednoznacznie, iż ww. warunki Wykonawca spełnił. 2. W przypadku gdy liczba Wykonawców, którzy złożyli niepodlegające odrzuceniu wnioski o dopuszczenie do udziału w postępowaniu, będzie mniejsza od 3 (trzech) Zamawiający ma trzy możliwości: 1) kontynuować postępowanie, zapraszając do składania ofert tych Wykonawców albo 2) zawiesić postępowanie i ponownie opublikować ogłoszenie o zamówieniu, określając, z zastosowaniem przepisów dotyczących terminów składania wniosków o dopuszczenie do udziału w postępowaniu, nowy termin składania wniosków oraz informując o tym Wykonawców, którzy spełniają warunki udziału w postępowaniu, albo 3) unieważnić postępowanie na podstawie art. 258 ust. 1 ustawy Pzp. 3. Zamawiający każdorazowo zaprosi

do składania ofert wszystkich Wykonawców, którzy spełniają warunki udziału w postępowaniu. Zamawiający nie formułuje żadnych kryteriów selekcji.

IV.1.3. Information about reduction of the number of solutions or tenders during negotiation or dialogue

IV.2. Award criteria

IV.2.1. Award criteria

Lowest price

IV.2.2. Information about electronic auction

An electronic auction has been used: no

IV.3. Administrative information

IV.3.1. File reference number attributed by the contracting authority

993200.271.37.2023

IV.3.2. Previous publication concerning this procedure

no

IV.3.3. Conditions for obtaining specifications and additional documents or descriptive document

IV.3.4. Time limit for receipt of tenders or requests to participate

7.11.2023 - 10:00

IV.3.5. Estimated date of dispatch of invitations to tender or to participate to selected candidates

IV.3.6. Languages in which tenders or requests to participate may be submitted

Polish.

Section VI: Complementary information

VI.1. Information about recurrence

This is a recurrent procurement: no

VI.2. Information about European Union funds

The procurement is related to a project and/or programme financed by European Union funds:
no

VI.3. Additional information

I. INFORMACJA O ZAMAWIAJĄCYM

1. Zamawiającym jest Zakład Ubezpieczeń Społecznych z siedzibą w Warszawie, ul. Szamocka 3, 5,
01-748 Warszawa, tel.: +48 22 667 17 04, NIP: 521-30-17-228, REGON 000017756,
strona internetowa – www.zus.pl.

adres poczty elektronicznej: SekretariatDZP@zus.pl

tel. : +48 22 667 17 04, godz. 7:30 – 15:30

2. Strona internetowa prowadzonego postępowania: <https://portal.smartpzp.pl/zus>

Strona internetowa, na której udostępniane będą zmiany, wyjaśnienia treści Wniosku o dopuszczenie do udziału w postępowaniu oraz wymiana informacji, przekazywanie dokumentów lub oświadczeń, innych dokumentów zamówienia bezpośrednio związanych z

postępowaniem o udzielenie zamówienia, odbywa się przy użyciu środków komunikacji elektronicznej zapewnionych przez Platformę zakupową, umożliwiającą obsługę procesu udzielania zamówień publicznych za pośrednictwem środków komunikacji elektronicznej:
<https://portal.smartpzp.pl/zus>

3. Postępowanie oznaczone jest znakiem 993200.271.37.2023 - Wykonawcy winni we wszelkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.
4. Przeglądanie i pobieranie publicznej treści dokumentacji postępowania nie wymaga posiadania konta na Platformie zakupowej, ani logowania do Platformy zakupowej.
5. Za pośrednictwem posiadanego na Platformie zakupowej konta Użytkownika Zewnętrznego tj. użytkownika Wykonawcy, odbywa się komunikacja Wykonawcy z Zamawiającym w postępowaniu, w szczególności: przekazywanie dokumentów, oświadczeń, informacji, pytań, wniosków w ramach postępowania.
6. Do korzystania z Platformy zakupowej przez Użytkowników Zewnętrznych konieczne jest posiadanie przez co najmniej jednego uprawnionego Użytkownika Zewnętrznego Wykonawcy kwalifikowanego podpisu elektronicznego służącego do autentykacji i podpisu. Korzystanie z Platformy zakupowej możliwe jest pod warunkiem spełnienia przez sprzęt, z którego korzystają użytkownicy Wykonawcy następujących minimalnych wymagań technicznych i specyfikacji połączenia:
 - posiadanie komputera o parametrach umożliwiających zainstalowanie następującego oprogramowania:
 - 1) w zakresie podstawowych funkcjonalności – przegląd, pobieranie i załączanie dokumentów:
 - a) komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min. 3 GB RAM, procesor 1500 MHz lub lepszy, jeden z systemów operacyjnych Linux Kernel 4.0, Windows 7 i MacOS 10.12 - lub ich nowsze wersje,
 - b) przeglądarka internetowa Mozilla Firefox ver. 65 i późniejsze, Google Chrome ver. 66 i późniejsze lub Opera w ver. 58 i późniejsze, Microsoft Edge ver 18 i późniejsze, Internet Explorer 11,
 - c) lista zalecanych przeglądarek internetowych: Google Chrome, Mozilla Firefox, Opera. Zalecane jest używanie najnowszych wersji przeglądarek,
 - 2) w zakresie składania podpisu kwalifikowanego (za pośrednictwem Platformy zakupowej):
 - a) zainstalowane środowisko Java w wersji min. 1.8 (jre),
 - b) w przypadku przeglądarek Opera, Chrome i Firefox należy doinstalować dodatek do przeglądarki Szafir SDK Web,
 - c) oprogramowania SzafirHost w systemie operacyjnym.
- Instrukcja instalowania oprogramowania wskazanego w punkcie 1) lit. a, b i c powyżej znajduje się na Platformie zakupowej w zakładce E-learning.
7. Korzystanie z Platformy zakupowej przez Wykonawców jest bezpłatne.
8. W sytuacji awarii Platformy zakupowej lub niedostępności Platformy zakupowej, uniemożliwiających komunikację Wykonawcy i Zamawiającego poprzez Platformę zakupową, Zamawiający dopuszcza komunikację za pomocą poczty elektronicznej na adres: SekretariatDZP@zus.pl (nie dotyczy składania Wniosków o dopuszczenie do udziału o zamówieniu). Wnioski o dopuszczenie do udziału w postępowaniu będą składane się wyłącznie w formie pisemnej w siedzibie Zamawiającego lub elektronicznej poprzez Platformę zakupową.
9. Maksymalny rozmiar pojedynczych plików przesyłanych za pośrednictwem Platformy zakupowej wynosi 100 MB. Za pośrednictwem Platformy zakupowej można przesłać wiele pojedynczych plików lub plik skompresowany do archiwum (ZIP) zawierający wiele pojedynczych plików.
10. Dopuszczalne formaty przesyłanych danych tj. plików o wielkości do 100 MB w formatach .png, .jpg, .jpeg, .gif, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .ods, .odp, .odf, .pdf, .zip, .rar, .

7zip, .txt, .ath, .xml, .dwg, .xades, .tar, .7z, .eml, .msg.

11. W przypadku, gdy wiadomość obejmuje informację niejawną, komunikacja odbywa się zgodnie z przepisami ustawy o ochronie informacji niejawnych.

II. WNIOSKI O DOPUSZCZENIE DO UDZIAŁU W POSTĘPOWANIU

1. Wykonawcy zainteresowani udziałem w postępowaniu winni złożyć Wniosek o dopuszczenie do udziału w postępowaniu. Każdy Wykonawca może przedstawić tylko jeden Wniosek o dopuszczenie do udziału w postępowaniu. Złożenie więcej niż jednego Wniosku o dopuszczenie do udziału w postępowaniu spowoduje odrzucenie wszystkich Wniosków złożonych przez Wykonawcę.

Wniosek o dopuszczenie do udziału w postępowaniu (dalej „Wniosek”) powinien być sporządzony w języku polskim, z zachowaniem formy (zgodnie z wyborem Wykonawcy):

1) pisemnej podpisanej własnoręcznym podpisem przez osobę upoważnioną do reprezentowania Wykonawcy;

2) elektronicznej w szczególności w formacie danych .pdf, .doc, .docx, .rtf, .xps, .odt, i podpisana kwalifikowanym podpisem elektronicznym przez osobę (-y) upoważnioną (-e) do reprezentowania Wykonawcy.

2. Każdy dokument składający się na Wniosek lub złożony wraz z Wnioskiem sporządzony w języku innym niż polski musi być złożony wraz z tłumaczeniem na język polski. Wniosek należy złożyć w oryginale. Wniosek uważa się za złożony w terminie, jeżeli dotarł do adresata przed upływem wyznaczonego terminu składania Wniosków o dopuszczenie do udziału w postępowaniu.

3. WNIOSKI O DOPUSZCZENIE DO UDZIAŁU W POSTĘPOWANIU MOŻNA SKŁADAĆ:

1) w formie pisemnej w siedzibie Zamawiającego w Warszawie na adres: Zakład Ubezpieczeń Społecznych, Departament Zamówień Publicznych, 01-748 Warszawa, ul. Szamocka 3, 5. Wniosek należy złożyć w zamkniętej kopercie. Kopertę należy oznaczyć w następujący sposób:

„Zakład Ubezpieczeń Społecznych, Departament Zamówień Publicznych, 01-748 Warszawa, ul. Szamocka 3, 5. Przetarg ograniczony „Wniosek o dopuszczenie do udziału w postępowaniu na „Świadczenie usług wsparcia eksploatacji i utrzymania Systemu Bezpieczeństwa Teleinformatycznego ZUS” nr postępowania: 993200.271.37.2023., nie otwierać przed 07.11.2023r., do godz. 10:00”.

Wniosek musi być napisany w języku polskim, na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką oraz podpisany przez osobę(y) upoważnioną do reprezentowania Wykonawcy na zewnątrz i zaciągania zobowiązań. Zaleca się, aby każda zapisana strona wniosku była ponumerowana kolejnymi numerami, a cały wniosek wraz z załącznikami był w trwały sposób ze sobą połączony (np. zbindowana, zszyta uniemożliwiając jej samoistną dekompletację), oraz zawierał spis treści. Zamawiający nie ponosi odpowiedzialności za wnioski złożone w innym miejscu niż wskazane w treści Ogłoszenia o zamówieniu. Na kopercie należy umieścić w postaci firmowej pieczęci lub odręcznego napisu nazwę Wykonawcy i jego adres zgodnie z danymi rejestrowym (ewidencyjnymi). Koperta powinna być zamknięta i zabezpieczona przed otwarciem bez uszkodzenia, gwarantując zachowanie poufności jej treści – do upływu terminu otwarcia Wniosków.

2) w formie elektronicznej za pomocą Platformy zakupowej <https://portal.smartpzp.pl/zus>.

4. FORMA SKŁADANYCH OŚWIADCZEŃ I DOKUMENTÓW W PRZYPADKU WNIOSKÓW SKŁADANYCH W FORMIE ELEKTRONICZNEJ:

1) Wnioski o dopuszczenie do udziału w postępowaniu, oświadczenie, o którym mowa w art. 125 ust. 1 ustawy Pzp (załączniki do wniosku), podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Pzp, pełnomocnictwo, sporządza się w postaci elektronicznej. Pozostałe dokumenty, informacje i oświadczenia sporządza się w postaci elektronicznej lub jako tekst wpisany do wiadomości przekazywanej przy

użyciu środków komunikacji elektronicznej. Dokumenty elektroniczne przekazuje się przy użyciu środków komunikacji elektronicznej wskazanych przez Zamawiającego (platforma zakupowa: <https://portal.smartpzp.pl/zus>).

2) Wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust. 1 ustawy Pzp składa się pod rygorem nieważności w formie elektronicznej (tj. podpisane kwalifikowanym podpisem elektronicznym).

3) W przypadku, gdy podmiotowe środki dowodowe, inne dokumenty, lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania”, zostały wystawione przez upoważnione podmioty inne niż Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub podwykonawca, zwane dalej „upoważnionymi podmiotami”, jako dokument elektroniczny, przekazuje się ten dokument.

4) W przypadku, gdy podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Pzp, niewystawione przez upoważnione podmioty lub pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym.

5) Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w ppkt. 4), dokonuje w przypadku:

a) podmiotowych środków dowodowych – odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia lub podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;

b) pełnomocnictwa – mocodawca.

Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa powyżej może dokonać również notariusz

6) W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym.

7) Zamawiający żąda załączenia do Wniosku o dopuszczenie do udziału w postępowaniu Pełnomocnictwa (oryginał w postaci elektronicznej podpisany elektronicznym podpisem kwalifikowanym lub elektroniczna kopia dokumentu potwierdzona za zgodność z oryginałem przez mocodawcę lub notariusza) do podpisania Wniosku, o ile prawo do reprezentowania Wykonawcy nie wynika z innych dokumentów złożonych wraz z Wnioskiem. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, do Wniosku należy dołączyć pełnomocnictwo podpisane elektronicznym podpisem kwalifikowanym przez uprawnionych przedstawicieli pozostałych Wykonawców, upoważniające jednego z Wykonawców do reprezentowania pozostałych.

8) Jeżeli Wniosek zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r o zwalczaniu nieuczciwej konkurencji, Wykonawca, w celu zachowania poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku. Podczas dodawania załączników do Wniosku Wykonawca ma możliwość ustawienia ich jako jawne lub niejawne. W razie jednoczesnego wystąpienia w danym dokumencie lub oświadczeniu treści o charakterze jawnym i niejawnym, należy podzielić ten plik na dwa pliki i każdy z nich odpowiednio oznaczyć. Odpowiednie oznaczenie zastrzeżonej treści Wniosku spoczywa na Wykonawcy. Jawną część uzasadnienia zastrzeżenia tajemnicy przedsiębiorstwa należy złożyć w odrębnym pliku.

5. FORMA SKŁADANYCH OŚWIADCZEŃ I DOKUMENTÓW W PRZYPADKU KOMUNIKACJI PISEMNEJ.

- 1) Wnioski o dopuszczenie do udziału w postępowaniu, oświadczenie, o którym mowa w art. 125 ust. 1 ustawy Pzp (załączniki od 1 do 11 do Wniosku), podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy Pzp, sporządza się w postaci pisemnej.
- 2) Wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust. 1 ustawy Pzp składa się pod rygorem nieważności w formie pisemnej (oryginał).
- 3) Podmiotowe środki dowodowe składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem. Zamawiający zażąda przedstawienia oryginału lub notarialnie potwierdzonej kopii oświadczenia lub dokumentu wyłącznie wtedy, gdy przedstawiona przez Wykonawcę kserokopia będzie nieczytelna lub będzie budzić wątpliwości, co do jej prawdziwości.
- 4) Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, w zakresie dokumentów, które każdego z nich dotyczą. Poświadczenie za zgodność z oryginałem następuje w formie pisemnej.
- 5) Zamawiający żąda załączenia do wniosku o dopuszczenie do udziału w postępowaniu pełnomocnictwa (oryginał dokumentu lub kopia poświadczona przez mocodawcę lub notariusza) do podpisania wniosku o dopuszczenie do udziału w postępowaniu, o ile prawo do reprezentowania Wykonawcy nie wynika z innych dokumentów złożonych wraz z wnioskiem. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia do wniosku należy dołączyć pełnomocnictwo podpisane przez uprawnionych przedstawicieli pozostałych Wykonawców, upoważniające jednego z Wykonawców do reprezentowania pozostałych lub pełnomocnika.
- 6) W przypadku, gdy informacje zawarte we Wniosku, dokumentach lub oświadczeniach, stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Wykonawca powinien to wyraźnie zastrzec poprzez złożenie ich w osobnej kopercie wraz z jednoczesnym oznaczeniem „Załącznik stanowiący tajemnicę przedsiębiorstwa”. Następnie wraz dokumentami złożyć w kopercie wraz z Wnioskiem - dokumenty składane w formie pisemnej – powinny być podpisane odręcznym podpisem.

III. KOMUNIKACJA POMIĘDZY ZAMAWIAJĄCYM A WYKONAWCAMI

Zgodnie z art. 401 ust. 1 ustawy Pzp. w przedmiotowym postępowaniu komunikacja pomiędzy Zamawiającym a Wykonawcami odbywać się będzie elektronicznie za pomocą Platformy zakupowej: <https://portal.smartpzp.pl/zus>, a w przypadku awarii platformy na adres e-mail: SekretariatDZP@zus.pl, z zastrzeżeniem, że wnioski i oferty należy składać w formie pisemnej lub elektronicznej.

IV. Zgłoszenie wniosku o dopuszczenie do udziału w postępowaniu może nastąpić telefonicznie przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu. Wniosek uważa się za złożony w terminie, jeżeli przed upływem terminu składania wniosków o dopuszczenie do udziału w postępowaniu został on wysłany i Zamawiający otrzymał go nie później niż w terminie 14 dni od dnia upływu terminu składania wniosków.

V. ZASTRZEŻENIE OSOBISTEGO WYKONANIA ZAMÓWIENIA

1. Zamawiający zastrzega obowiązek osobistego wykonania przez Wykonawcę kluczowych zadań dotyczących świadczenia usługi w zakresie Integratora Bezpieczeństwa. Integrator Bezpieczeństwa jest to kluczowa funkcja realizowana przez Wykonawcę z udziałem dedykowanych osób określonych w Wykazie osób jako „Integratorzy bezpieczeństwa”, skierowanych do realizacji zamówienia / Umowy. Funkcja ta nie jest przypisana członkom zespołów projektowych.

2. Zakres zadań Integratora Bezpieczeństwa jest zastrzeżony do osobistego wykonania przez

Wykonawcę, a zatem Wykonawca musi samodzielnie spełniać warunki udziału w postępowaniu dla Integratora Bezpieczeństwa w zakresie doświadczenia wykonawcy oraz dysonowania osobami określanymi jako Integratorzy bezpieczeństwa. Nie dopuszcza się realizacji zamówienia w tym zakresie przy pomocy podwykonawców.

VI. DODAKOWE INFORMACJE - PRZEDMIOT ZAMÓWIENIA

1. Opis przedmiotu zamówienia, który zostanie przekazany Wykonawcom zaproszonym do składania ofert będzie zawierał:

- 1) informacje jawne,
- 2) informacje stanowiące tajemnicę Zakładu Ubezpieczeń Społecznych, których udostępnienie będzie wymagało uprzedniego zawarcia umowy o poufności; wzór umowy o zachowanie poufności zostanie przekazany wykonawcom wraz z zaproszeniem do składania ofert,
- 3) informacje niejawne o klauzuli „zastrzeżone”, które będą udostępniane zgodnie z ustawą o z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tekst jednolity (Dz.U. z 2023 r. poz. 756 z późn. zm.)).

2. Informacje niejawne będą przekazywane w formie elektronicznej. Nośnik danych zawierający informacje niejawne Wykonawca będzie mógł odebrać jedynie osobiście w siedzibie Zamawiającego. Osoba odbierająca nośnik danych zawierający informacje niejawne w siedzibie Zamawiającego będzie musiała przedstawić Zamawiającemu następujące dokumenty:

1) ważne poświadczenie bezpieczeństwa uprawniające do dostępu do informacji niejawnych o klauzuli tajności minimum „poufne” lub upoważnienie do dostępu do informacji niejawnej o klauzuli zastrzeżone,

2) aktualne zaświadczenie o odbytym szkoleniu w zakresie ochrony informacji niejawnych.

3. Udostępnienie informacji innym osobom w organizacji Wykonawcy wymaga zachowania procedur określonych w ustawie o ochronie informacji niejawnych, w tym może być udostępniane na zasadach adekwatności jedynie osobom legitymującym się dokumentami wskazanymi powyżej. Wykonawca jest zobowiązany do poinformowania wszystkich osób, w tym podwykonawców, którym przekaże informacje niejawne o ciążyącym na nich obowiązku ochrony informacji niejawnych.

4. Zamawiający nie zezwala na kopiowanie informacji niejawnych zawartych na nośniku danych przekazanym Wykonawcy. W przypadku gdyby z uwagi na szczególne okoliczności związane z przygotowaniem oferty wystąpiła konieczność dokonania kopii informacji niejawnych to Wykonawca jest zobowiązany złożyć Zamawiającemu wniosek o wykonanie dodatkowej/wych kopii wraz ze wskazaniem obiektywnych powodów oraz liczby kopii. Kopia informacji niejawnych zostanie wykonana przez Zamawiającego i przekazana Wykonawcy na nowym nośniku danych.

5. Wykonawca, którego oferta nie zostanie wybrana jako najkorzystniejsza w Postępowaniu zobowiązany jest w terminie 14 dni od uprawomocnienia się decyzji o wyborze oferty najkorzystniejszej zwrócić nośniki danych zawierające informacje niejawne przekazane przez Zamawiającego w toku Postępowania

VII. KLAUZULA INFORMACYJNA – ART. 13 RODO

1. Zamawiający jako administrator danych osobowych, obowiązany jest do spełnienia obowiązku informacyjnego z art. 13 RODO względem osób fizycznych, od których dane osobowe bezpośrednio pozyskał. Dotyczy to w szczególności:

- wykonawcy będącego osobą fizyczną,
- wykonawcy będącego osobą fizyczną, prowadzącą jednoosobową działalność gospodarczą,
- pełnomocnika wykonawcy będącego osobą fizyczną (np. dane osobowe zamieszczone w pełnomocnictwie),
- członek organu zarządzającego wykonawcy, będącego osobą fizyczną (np. dane osobowe zamieszczone w informacji z KRK),

- osoby fizycznej skierowanej do przygotowania i przeprowadzenia postępowania o udzielenie zamówienia publicznego.

2. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO”, Zamawiający informuje, że:

- administratorem Pani/Pana danych osobowych jest Zakład Ubezpieczeń Społecznych z siedzibą w Warszawie, ul. Szamocka 3, 5, 01-748 Warszawa;
- Zakład Ubezpieczeń Społecznych wyznaczył Inspektora Ochrony Danych. Może się Pani /Pan z nim kontaktować we wszystkich sprawach, które dotyczą przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych:

- listownie na adres:

Inspektor Ochrony Danych

ul. Szamocka 3, 5

01-748 Warszawa

- przez e-mail: ODO@zus.pl

- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego znak postępowania 993200.271.37.2023 na „Świadczenie usługi wsparcia eksploatacji i utrzymania Systemu Bezpieczeństwa Teleinformatycznego ZUS” oraz w celu spełnienia obowiązku prawnego wynikającego z przepisów ustawy;

- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ustawy;

- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ust. 1 i 4 ustawy, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy;

- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

- posiada Pani/Pan:

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;

- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych*;

- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO**;

- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani /Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

- nie przysługuje Pani/Panu:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;

- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;

- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

3. Zgodnie z wytycznymi Urzędu Zamówień Publicznych, Wykonawca powinien złożyć stosowne oświadczenie. Treść oświadczenia została zawarta w pkt 5 Wniosku o dopuszczenie do udziału w postępowaniu.

* Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku

postępowania

o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą oraz nie może naruszać integralności protokołu oraz jego załączników.

**** Wyjaśnienie:** prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

VI.4. Procedures for review

VI.4.1. Review body

Official name: Krajowa Izba Odwoławcza

Postal address: ul. Postępu 17a

Town: Warszawa

Postal code: 02-676

Country: Poland

E-mail: odwolania@uzp.gov.pl

Telephone: +48 224587801

Fax: +48 224587800

Internet address: <https://www.uzp.gov.pl/kio>

VI.4.2. Review procedure

Precise information on deadline(s) for review procedures: 1. Każdemu Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp przysługują środki ochrony prawnej przewidziane w dziale IX ustawy Pzp, jak dla postępowań o wartości równej albo przekraczającej progi unijne.

2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 ustawy Pzp oraz Rzecznikowi Małych i Średnich Przedsiębiorców.

3. Odwołanie przysługuje na:

3.1. niezgodną z przepisami ustawy Pzp czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;

3.2. zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy Pzp.

4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej.

5. Odwołujący przekazuje Zamawiającemu odwołanie wniesione w formie elektronicznej albo postaci elektronicznej albo kopię tego odwołania, jeżeli zostało ono wniesione w formie pisemnej, przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Odwołujący przesyła kopię odwołania Zamawiającemu poprzez Platformę zakupową – na adres: <https://portal.smartpzp.pl/zus> w ramach danego postępowania lub na adres: e-mail:

SekretariatDZP@zus.pl

6. Odwołanie wnosi się w terminie:

6.1. 10 dni od dnia przekazania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia, jeżeli informacja została przekazana przy użyciu środków komunikacji elektronicznej, albo w terminie 15 dni – jeżeli informacja została przekazana w inny sposób;

6.2. 10 dni od dnia publikacji ogłoszenia w Dzienniku Urzędowym Unii Europejskiej lub zamieszczenia dokumentów zamówienia na stronie internetowej – wobec treści ogłoszenia o zamówieniu oraz wobec dokumentów zamówienia;

6.3. 10 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było

powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia – wobec czynności innych niż określone w pkt 6.1 i 6.2 powyżej.

7. W przypadku wniesienia odwołania wobec treści ogłoszenia o zamówieniu lub dokumentów zamówienia Zamawiający może przedłużyć termin składania wniosków o dopuszczenie do udziału w postępowaniu/ofert.

VI.4.3. Service from which information about the review procedure may be obtained

Official name: Krajowa Izba Odwoławcza

Postal address: ul. Postępu 17a

Town: Warszawa

Postal code: 02-676

Country: Poland

E-mail: odwolania@uzp.gov.pl

Telephone: +48 224587801

Fax: +48 224587800

Internet address: <https://www.uzp.gov.pl/kio>

VI.5. Date of dispatch of this notice

3.10.2023