Ciechanów, dnia 31.03.2026 r.

Powiat Ciechanowski
z siedzibą w Ciechanowie
ul. 17 Stycznia 7
06-400 Ciechanów

WRI-ZP.272.3.6.2026

Do Wykonawców
biorących udział w postępowaniu

Dotyczy postępowania pn.:
„Dostawa środowiska kopii bezpieczeństwa" w ramach realizacji Umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/1491/ FERC.02.02-CS.01-001/23/2024 „Cyberbezpieczny Samorząd"; Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa.

Szanowni Państwo!

Na podstawie art. 284 ust. 2 ustawy z dnia 11 września 2019 r Prawo zamówień publicznych (Dz. U. z 2024 poz. 1320 ze zm.) dalej jako „ustawa Pzp", Zamawiający w niniejszym postępowaniu o udzielenie zamówienia publicznego, przekazuję treść pytań wraz z odpowiedziami:

Pytanie Wykonawcy nr 1:
„Wnosimy o dopuszczenie realizacji wskazanych w OPZ prac w trybie zdalnym, przy zapewnieniu przez Wykonawcę bezpiecznego dostępu (np. VPN, szyfrowane protokoły, tunelowanie, MFA).
Po analizie opisu przedmiotu zamówienia zauważamy, że część czynności wymaga obecności na miejscu wyłącznie w przypadkach uzasadnionych (np. montaż sprzętu, instalacje fizyczne w szafach Rack, doposażenie serwerów). Natomiast pozostałe prace – w szczególności instalacje logiczne, konfiguracje systemów, wdrożenia oprogramowania, testy, migracje, budowa polityk, integracje, konfiguracje logów, systemów SIEM/XDR, monitoringu oraz szkolenia – mogą być w całości wykonane zdalnie, bez wpływu na jakość wdrożenia ani ciągłość pracy Urzędu.
Wymóg realizacji wszystkich etapów w trybie stacjonarnym istotnie ogranicza konkurencję oraz stoi w sprzeczności z powszechną praktyką rynkową wdrożeń systemów backupu, SIEM/XDR, logów oraz monitoringu, które standardowo prowadzone są zdalnie.
W załączeniu (lub poniżej – zależnie od formy przekazania Zamawiającemu) przedstawiamy tabelaryczne zestawienie prac z OPZ wraz z proponowanym trybem ich realizacji:
– prace wymagające fizycznej obecności (montaż, doposażenie),
– prace możliwe do wykonania zdalnie, przy zachowaniu pełnego bezpieczeństwa.

Zwracamy się zatem z pytaniem:
Czy Zamawiający dopuści realizację prac wskazanych w załączonej tabeli w trybie zdalnym, z zachowaniem odpowiednich mechanizmów bezpieczeństwa?

Rozdział OPZ	Co dokładnie trzeba zrobić	Tryb realizacji
1	Opracowanie koncepcji środowiska backupu: 3-2-1-1-0, WORM, RTO/RPO, okna serwisowe, opis fizycznych i logicznych połączeń, segmentacja sieci backupowej, sposób postępowania z taśmami, uwzględnienie logów i monitoringu	**Zdalnie**
2	Dostarczenie serwera backupowego, macierzy, urządzenia taśmowego i interfejsów dla serwerów produkcyjnych	**Stacjonarnie**
3	Montaż serwera w szafie Rack, wstępna konfiguracja interfejsu zarządzania, konfiguracja RAID1 na system i RAID5 na dane, instalacja systemu, sterowników i aktualizacji, podłączenie do sieci po SFP28	**Stacjonarnie** — część prac inżynieryjnych z rozdz. 3
3	Montaż macierzy w Rack, wstępna konfiguracja zarządzania, podłączenie do sieci po SFP28, RAID5, utworzenie udziału sieciowego pod Acronisa	**Stacjonarnie** — część prac inżynieryjnych z rozdz. 3
3	Montaż biblioteki/napędu w Rack, wstępna konfiguracja zarządzania, podłączenie do serwera, inicjalizacja taśm LTO9	**Stacjonarnie** — część prac inżynieryjnych z rozdz. 3
2.4 i 3	Instalacja i konfiguracja dodatkowych interfejsów 10Gb w serwerach produkcyjnych 1 i 2, wkładki i światłowody	**Stacjonarnie**
3	Instalacja serwera zarządzania Acronis Cyber Protect Backup na dostarczonym serwerze	**Zdalnie** po fizycznym uruchomieniu serwera i dostępie VPN/TeamViewer
3	Przeniesienie obecnych licencji Acronisa do nowego serwera zarządzania	**Zdalnie**
3	Reinstalacja agentów Acronis i przepięcie relacji zarządzania do nowego serwera	**Zdalnie**
3	Inwentaryzacja maszyn wirtualnych wymagających ochrony	**Zdalnie**
3	Konfiguracja magazynów kopii: lokalne dyski serwera zarządzania, zasób SMB z macierzy, urządzenie taśmowe	**Zdalnie**
3	Definicja planu krótkoterminowego na macierzy z możliwie częstym wykonywaniem kopii	**Zdalnie**
3	Definicja planu długoterminowego na lokalnych zasobach serwera i na taśmie, z możliwie długim przechowywaniem	**Zdalnie**
4	Instalacja systemu operacyjnego na VM Hyper-V przeznaczonej pod centralny system logów	**Zdalnie**
4	Weryfikacja źródeł czasu na urządzeniach i systemach wysyłających logi oraz propozycja uspójnienia czasu w sieci	**Zdalnie**
4	Instalacja rozwiązania, konfiguracja podstawowych parametrów pracy i polityk dostępu dla informatyków	**Zdalnie**
4	Konfiguracja retencji danych zgodnie z aktami prawnymi i dobrymi praktykami	**Zdalnie**
4	Konfiguracja wysyłania logów z: 1× Stormshield, 10× Netgear, 9× Windows Server, 3× Linux, 130× Windows 10/11, 1× ESET, 3× Hyper-V, 1× Axence nVision, 1× Vutlan	**Zdalnie** — razem 159 źródeł logów
4	Zdefiniowanie portów nasłuchu i segmentacji źródeł logów	**Zdalnie**
4	Wstępna analiza logów i przygotowanie ekstraktorów	**Zdalnie**
4	Rekonfiguracja Axence nVision tak, aby przesyłał logi i alarmy do centralnego systemu logów	**Zdalnie**
4	Budowa dashboardów, reguł alarmowych i powiadomień	**Zdalnie**
4	Konfiguracja wysyłki powiadomień przez mail lub Microsoft Teams	**Zdalnie**
4 i 8	Wprowadzenie informatyków do obsługi systemu	**Zdalnie** — OPZ wymaga szkolenia, ale nie wskazuje, że ma być na miejscu

CENTRUM PROJEKTÓW POLSKA CYFROWA I
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.p

4.3	12 miesięcy zdalnej pomocy, aktualizacji i obsługi zgłoszeń w godz. 8–16	**Zdalnie**
5	Instalacja systemu operacyjnego pod SIEM/XDR na wskazanym serwerze/VM	**Zdalnie**
5	Instalacja rozwiązania, konfiguracja podstawowych parametrów i polityk dostępu	**Zdalnie**
5	Konfiguracja retencji danych według polityk bezpieczeństwa Zamawiającego	**Zdalnie**
5	Konfiguracja mechanizmów powiadamiania o zagrożeniach przez e-mail	**Zdalnie**
5	Wdrożenie monitorowania/agenta na 12× Windows Server, 3× Linux, 130× Windows 10/11	**Zdalnie** — razem 145 końcówek
5	Zdefiniowanie mechanizmów oceny konfiguracji zgodnie z CIS Control	**Zdalnie**
5	Zdefiniowanie wykrywania podatności systemów i aplikacji zgodnie z CVE MITRE	**Zdalnie**
5	Konfiguracja SCA, Rootchecks i FIM do wykrywania złośliwego oprogramowania	**Zdalnie**
5	Konfiguracja analizy logów w oparciu o MITRE ATT&CK	**Zdalnie**
5	Korelacja danych między SIEM/XDR a centralnym systemem logów	**Zdalnie**
5 i 8	Szkolenie z codziennego wykorzystania systemu SIEM/XDR	**Zdalnie** — OPZ nie narzuca onsite
5.3	12 miesięcy zdalnej pomocy, aktualizacji i obsługi zgłoszeń w godz. 8–16	**Zdalnie**
6	Instalacja systemu operacyjnego na serwerze lub maszynie wirtualnej	**Zdalnie**
6	Weryfikacja źródeł czasu na urządzeniach i systemach objętych monitoringiem	**Zdalnie**
6	Instalacja rozwiązania, konfiguracja podstawowych parametrów i polityk dostępu	**Zdalnie**
6	Konfiguracja retencji danych zgodnie z aktami prawnymi i dobrymi praktykami	**Zdalnie**
6	Rejestracja urządzeń: 1× Stormshield, 10× Netgear, 9× Windows Server, 3× Linux, 130× Windows 10/11, 3× Hyper-V	**Zdalnie** — razem 156 urządzeń
6	Dopasowanie gotowych szablonów albo opracowanie własnych wzorców monitoringu	**Zdalnie**
6	Budowa dashboardów analitycznych i tematycznych	**Zdalnie**
6	Przygotowanie zbiorczego pulpitu do wyświetlania 24/7 na ekranie informatyków	**Zdalnie**; fizyczne sprawdzenie ekranu może zrobić lokalny pracownik
6	Konfiguracja mechanizmów alarmowania i powiadomień	**Zdalnie**
6	Konfiguracja wysyłki powiadomień przez mail lub Microsoft Teams	**Zdalnie**
6 i 8	Szkolenie z zarządzania i administracji monitoringiem	**Zdalnie**
6.9	12 miesięcy zdalnej pomocy, aktualizacji i obsługi zgłoszeń w godz. 8–16	**Zdalnie**
7	Wykonanie kopii każdej chronionej maszyny wirtualnej, w każdym planie i do każdego magazynu	**Zdalnie** przy pełnym dostępie administracyjnym
7	Testowe odtworzenie każdej utworzonej kopii; poza godzinami pracy urzędu albo niekolidująco z produkcją	**Zdalnie** przy pełnym dostępie administracyjnym
8	Szkolenia dla informatyków obejmujące wszystkie dostarczone i wdrożone elementy	**Zdalnie**
9	Opracowanie dokumentacji końcowej środowiska kopii bezpieczeństwa	**Zdalnie**

”

CENTRUM PROJEKTÓW POLSKA CYFROWA I
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.p

Odpowiedź Zamawiającego:
Zamawiający informuje, że nie dokonuje zmian w Opisie przedmiotu zamówienia – załącznik nr 5 do SWZ. Zadane pytanie dotyczy etapu realizacji zamówienia, i jego technicznych uwarunkowań – co będzie ustalane po podpisaniu umowy, na podstawie dokumentów składanych przez wykonawcę.

Zamawiający informuje, że ulega zmianie termin składania i otwarcia ofert. Oferty należy składać do dnia 10.04.2026 r. do godz. 10:00. Otwarcie ofert nastąpi w dniu 10.04.2026r. o godz. 11:00. W konsekwencji zmianie ulega termin związania ofertą z dnia 30.04.2026 r. do dnia 09.05.2026 r.

Analogicznej zmianie ulegają postanowienia SWZ rozdz. III podrozdz. 2 i 3 oraz ogłoszenie o zamówieniu nr 2026/BZP 00162892 z dnia 19.03.2026 r.

/-/ Kierownik Zamawiającego

CENTRUM PROJEKTÓW POLSKA CYFROWA I
ul. Spokojna 13A, 01-044 Warszawa | infolinia: +48 223152340 | e-mail: cppc@cppc.gov.p