DINF-WIT.26.8.2026

Odpowiedzi na pytania 4-13
Testy bezpieczeństwa

Pytanie nr 4:
Pytanie – zakres ilościowy Części I Pkt 3 ust. 2 OPZ przewiduje testy „wybranych, reprezentatywnych hostów w sieci wewnętrznej" oraz „wybranych segmentów sieci wewnętrznej", nie określając ich liczby. Prosimy o wskazanie szacunkowej liczby hostów (serwerów, urządzeń sieciowych, urządzeń bezpieczeństwa) oraz segmentów sieci wewnętrznej objętych testami.
Prosimy także o potwierdzenie, że zakres ustalany w RoE nie przekroczy wskazanych wartości. Informacja ta jest niezbędna do rzetelnej wyceny ryczałtowej oraz zaplanowania prac w terminie do 17 grudnia 2026 r.

Odpowiedź na pytanie nr 4:
Zgodnie z opublikowaną odpowiedzią na pytanie nr 1 Zamawiający przewiduje objęcie testami infrastruktury wewnętrznej 12 adresów IP, obejmujących wybrane serwery, urządzenia sieciowe, urządzenia bezpieczeństwa (appliance), urządzenia peryferyjne oraz stacje robocze.
Testy obejmą wybrane segmenty sieci wewnętrznej. Ich liczba, dobór oraz szczegółowe scenariusze i sposób dostępu zostaną uzgodnione z Wykonawcą na etapie przygotowania i zatwierdzenia RoE, przy zachowaniu wskazanej liczby 12 adresów IP objętych testami wewnętrznymi.
Nie przewiduje się pełnego skanowania wszystkich hostów w poszczególnych segmentach.
Zakres zewnętrzny pozostaje odrębny i obejmuje jeden uzgodniony zakres publicznej adresacji IPv4 nie większy niż /24.

Pytanie nr 5:
Pytanie – wielkość Serwisów WWW w Części II Prosimy o podanie dla każdego z 6 Serwisów WWW następujących informacji:
a) szacunkowej liczby podstron lub widoków funkcjonalnych;
b) liczby formularzy oraz szacunkowej łącznej liczby pól wejściowych (parametrów przekazywanych przez użytkownika);
c) liczby endpointów API (REST/SOAP/GraphQL) wraz ze wskazaniem, czy dostępna jest dokumentacja API (np. specyfikacja OpenAPI/Swagger);
d) informacji, czy Serwis posiada mechanizm logowania i ile ról użytkowników przewiduje;
e) informacji, czy Serwis udostępnia funkcje przesyłania plików lub panel administracyjny;
f) wykorzystywanej technologii, w tym informacji, czy Serwis jest oparty na systemie CMS (np. WordPress, Drupal).

Odpowiedź na pytanie nr 5:
Ad a) Zamawiający nie określa obecnie liczby podstron ani widoków funkcjonalnych dla poszczególnych Serwisów WWW. Zgodnie z odpowiedzią na pytanie nr 2 przedmiotem testów jest 6 Serwisów dostępnych pod 6 adresami FQDN, bez dodatkowych subdomen. Każdy Serwis może obejmować odrębne aplikacje pod dodatkowymi ścieżkami URL; informacje o znanych aplikacjach zostaną przekazane po zawarciu umowy, a identyfikacja pozostałych ścieżek stanowi element Fazy 1 – rekonesansu black-box.

Departament Informatyzacji
Telefon: +48 22 577 51 70
e-mail: sekretariatdinf@gios.gov.pl
ul. Chmielna 132/134, 00-805 Warszawa
Główny Inspektorat Ochrony Środowiska

Ad b) W zakresie liczby formularzy i pól wejściowych odpowiedzi udzielono już w ramach odpowiedzi na pytanie nr 3 (Ad 3).

Ad c) W zakresie liczby punktów API odpowiedzi udzielono już w ramach odpowiedzi na pytanie nr 2. Informacje o dostępnej dokumentacji API, o ile Zamawiający nią dysponuje, zostaną przekazane Wykonawcy po zawarciu umowy, na etapie przygotowania RoE.

Ad d) W zakresie mechanizmów uwierzytelniania oraz liczby ról użytkowników odpowiedzi udzielono już w ramach odpowiedzi na pytanie nr 3 (Ad 2).

Ad e) Informacje o dostępności funkcji przesyłania plików oraz paneli administracyjnych w poszczególnych Serwisach, w zakresie znanym Zamawiającemu, zostaną przekazane Wykonawcy po zawarciu umowy, na etapie przygotowania RoE. Identyfikacja pozostałych funkcjonalności stanowi element Fazy 1 – rekonesansu.

Ad f) W zakresie ogólnej charakterystyki aplikacji odpowiedzi udzielono już w ramach odpowiedzi na pytanie nr 3 (Ad 1). Szczegółowe informacje o wykorzystywanych technologiach, w zakresie znanym Zamawiającemu, zostaną przekazane Wykonawcy po zawarciu umowy. Identyfikacja publicznie dostępnych komponentów i technologii stanowi również element Fazy 1 – rekonesansu, zgodnie z pkt 4.1 OPZ.

Pytanie nr 6:

Pytanie – krytyczność Serwisów i środowisko testowe Zgodnie z pkt 4.3 ust. 2 OPZ dla Serwisów o krytyczności wysokiej i krytycznej wymagana jest dodatkowo weryfikacja wybranych wymagań OWASP ASVS Level 2. Prosimy o wskazanie, ile z 6 Serwisów Zamawiający kwalifikuje jako normalne, wysokie i krytyczne. Prosimy również o informację, dla których Serwisów (oraz zasobów Części I) dostępne jest reprezentatywne środowisko testowe (mirror).

Odpowiedź na pytanie nr 6:

Ad 1. Zamawiający nie określa na tym etapie liczbowego podziału 6 Serwisów na poziomy krytyczności normalny, wysoki i krytyczny. Klasyfikacja zostanie wskazana w RoE z uwzględnieniem rodzaju i funkcjonalności Serwisów oraz przetwarzanych danych. Zgodnie z pkt 4.3 OPZ dla Serwisów o normalnej krytyczności stosuje się adekwatne wymagania ASVS Level 1, a dla Serwisów o wysokiej lub krytycznej krytyczności dodatkowo wybrane wymagania ASVS Level 2, uzgodnione przed Fazą 2. Szczegółowe przypisanie krytyczności oraz adekwatnych scenariuszy testowych zostanie uzgodnione na etapie opracowania RoE, zgodnie z OPZ.

Ad 2. Dostępność reprezentatywnych środowisk testowych (mirror) dla poszczególnych zasobów Części I i Serwisów Części II zostanie zweryfikowana i uzgodniona na etapie przygotowania RoE. Zamawiający nie gwarantuje dostępności odrębnego mirroru dla każdego badanego zasobu. Zasady bezpiecznych testów na produkcji i odrębnych zgód na scenariusze podwyższonego ryzyka określa pkt 6 OPZ.
W zakresie uzgadniania terminów prowadzenia testów i dostępności środowisk Zamawiający udzielił już odpowiedzi na pytanie nr 1 (Ad 2).
Zasady wykorzystania środowisk produkcyjnych i testowych, w tym ograniczenia dotyczące scenariuszy podwyższonego ryzyka, określa pkt 6 OPZ. Szczegółowe warunki przeprowadzenia testów zostaną uzgodnione w RoE.

Pytanie nr 7:

Pytanie – wpływ opóźnień po stronie Zamawiającego na termin realizacji § 3 ust. 2 pkt 2 projektowanych postanowień umowy (PPU) wyznacza termin 17 grudnia 2026 r. Termin ten nie zależy od momentu przekazania przez Zamawiającego danych wejściowych, kont testowych i dostępów ani od zatwierdzenia RoE. Prosimy o potwierdzenie, że opóźnienie po stronie Zamawiającego w tym zakresie spowoduje odpowiednie przesunięcie terminu realizacji i nie będzie podstawą do naliczenia kar umownych. Jeśli Zamawiający tego nie potwierdza, prosimy o rozważenie odpowiedniej modyfikacji PPU.

Odpowiedź na pytanie nr 7:

Zamawiający przewiduje współdziałanie z Wykonawcą przy przygotowaniu RoE oraz przekazanie posiadanych danych i dostępów niezbędnych do realizacji uzgodnionych testów, na zasadach określonych w PPU. Szczegółowa organizacja i harmonogram udostępniania zostaną uzgodnione niezwłocznie po zawarciu umowy.

Zgodnie z § 5 ust. 3–4 PPU Zamawiający udostępnia informacje i dostępy w uzgodnionych terminach, a Wykonawca jest zobowiązany do niezwłocznego zgłaszania okoliczności mogących wpłynąć na terminowość realizacji zamówienia, wraz z określeniem ich przyczyn, skutków i proponowanych rozwiązań.

Zamawiający wskazuje, że kary umowne przewidziane w § 13 ust. 2 pkt 2 PPU dotyczą zwłoki Wykonawcy, a nie każdego przypadku opóźnienia. W konsekwencji opóźnienia wynikające wyłącznie z przyczyn leżących po stronie Zamawiającego, za które Wykonawca nie ponosi odpowiedzialności, nie będą stanowiły podstawy do naliczenia kar umownych z tego tytułu.

Jednocześnie termin zakończenia realizacji zamówienia wskazany w dokumentacji pozostaje bez zmian. Zamawiający nie przewiduje jego automatycznego przedłużenia z uwagi na opóźnienia organizacyjne.

Pytanie nr 8:

Pytanie – skutki zgłoszenia uwag w procedurze odbioru Zgodnie z § 10 ust. 11 PPU, jeżeli Zamawiający stwierdzi błędy w produktach zgłoszonych do odbioru, termin uważa się za niedotrzymany. Wówczas termin wykonania przesuwa się na dzień przekazania produktów bez uwag, co skutkuje naliczeniem kar umownych. Prosimy o modyfikację tego postanowienia tak, aby usunięcie uwag w terminie wskazanym w § 10 ust. 6 PPU nie powodowało uznania terminu za niedotrzymany. Dotyczy to w szczególności uwag zgłoszonych do wersji roboczej raportu przekazanej zgodnie z § 3 ust. 4 PPU.

Odpowiedź na pytanie nr 8:

Należy rozróżnić zgłaszanie uwag do roboczej wersji raportów i materiałów odbiorowych, o której mowa w § 3 ust. 4 PPU, od formalnej procedury odbioru określonej w § 10 PPU.

Uwagi zgłaszane do wersji roboczej mają na celu umożliwienie Wykonawcy wprowadzenia niezbędnych uzupełnień i korekt przed przekazaniem dokumentacji końcowej. Samo zgłoszenie takich uwag nie stanowi podstawy do uznania terminu realizacji zamówienia za niedotrzymany ani do naliczenia kar umownych.

W odniesieniu do formalnej procedury odbioru Zamawiający podtrzymuje postanowienia § 10 PPU. Procedura zgłaszania i usuwania niezgodności nie stanowi automatycznego przedłużenia terminu realizacji określonego w § 3 ust. 2 pkt 2 PPU.

Jednocześnie należy wskazać, że kary umowne przewidziane w § 13 ust. 2 pkt 2 PPU dotyczą zwłoki Wykonawcy, a ich naliczenie następuje z uwzględnieniem okoliczności i przyczyn niedotrzymania terminu.

Zamawiający nie przewiduje modyfikacji PPU w tym zakresie.

Pytanie nr 9:

Pytanie – ograniczenie odpowiedzialności odszkodowawczej Ze względu na charakter usługi (aktywne testy bezpieczeństwa, również na środowisku produkcyjnym) prosimy o rozważenie ograniczenia łącznej odpowiedzialności odszkodowawczej Wykonawcy z tytułu Umowy do wysokości wynagrodzenia brutto za daną Część. Ograniczenie nie dotyczyłoby szkód wyrządzonych umyślnie. Dotyczy to § 5 ust. 5 i 7 oraz § 13 ust. 9 PPU.

Odpowiedź na pytanie nr 9:
Nie przewiduje się wprowadzenia proponowanego ograniczenia łącznej odpowiedzialności odszkodowawczej Wykonawcy do wysokości wynagrodzenia brutto za daną Część zamówienia.

Zamawiający uwzględnia charakter testów prowadzonych również na środowisku produkcyjnym. Z tego względu OPZ i PPU przewidują uzgadnianie RoE, odrębne zgody na scenariusze podwyższonego ryzyka i możliwość wstrzymania testów. Mechanizmy te służą ograniczeniu ryzyka po obu stronach, bez zmiany obowiązujących zasad odpowiedzialności.

Jednocześnie Zamawiający wskazuje, że OPZ oraz § 6 i § 7 PPU przewidują mechanizmy ograniczania ryzyka związanego z prowadzeniem testów, w szczególności uzgadnianie zakresu i warunków testów w ramach RoE, odrębne zatwierdzanie scenariuszy podwyższonego ryzyka oraz możliwość wstrzymania testów.

Odpowiedzialność odszkodowawcza Wykonawcy podlega zasadom określonym w Umowie oraz właściwych przepisach prawa.

Zamawiający podtrzymuje dotychczasowe postanowienia PPU w tym zakresie.

Pytanie nr 10:
Pytanie – charakter wynagrodzenia § 11 ust. 5 PPU określa wynagrodzenie jako ryczałtowe, natomiast § 11 ust. 10 PPU stanowi, że „wypłata wynagrodzenia nastąpi za faktycznie wykonaną pracę". Prosimy o wyjaśnienie relacji między tymi postanowieniami. Prosimy też o potwierdzenie, że nieprzeprowadzenie scenariuszy, na które Zamawiający nie wyraził zgody (§ 6 ust. 2 PPU, pkt 6 ust. 3 OPZ), nie spowoduje obniżenia wynagrodzenia ryczałtowego.

Odpowiedź na pytanie nr 10:
Wynagrodzenie za realizację każdej Części zamówienia ma charakter ryczałtowy, zgodnie z § 11 ust. 1 i 5 PPU.

Postanowienie § 11 ust. 9 PPU, odnoszące się do faktycznie wykonanej pracy, nie oznacza rozliczania Wykonawcy według liczby przeprowadzonych scenariuszy testowych, przepracowanych godzin ani nakładu pracy, lecz odnosi się do należytego wykonania i odbioru danej Części zamówienia zgodnie z Umową, OPZ oraz zatwierdzonym RoE.

Potwierdzamy, że nieprzeprowadzenie scenariuszy podwyższonego ryzyka, na których realizację Zamawiający nie wyraził zgody, nie będzie samo w sobie stanowiło podstawy do obniżenia wynagrodzenia ryczałtowego, pod warunkiem prawidłowego wykonania pozostałego wymaganego zakresu testów oraz udokumentowania niewykonanych scenariuszy i przyczyn ich pominięcia w raporcie końcowym i macierzy pokrycia, zgodnie z OPZ.

Powyższe nie zwalnia Wykonawcy z obowiązku wykonania wszystkich pozostałych czynności objętych zamówieniem ani nie stanowi podstawy do samodzielnego ograniczania zakresu testów przez Wykonawcę.

Pytanie nr 11:
Pytanie – lokalizacja infrastruktury narzędzi testowych § 15 ust. 3 PPU odnosi się do „wymaganych w OPZ narzędzi działających z serwerów centrum danych na terytorium Polski", natomiast pkt 12 ust. 3 OPZ wymaga zgody Zamawiającego wyłącznie na przetwarzanie informacji poza EOG. Prosimy o wyjaśnienie, czy infrastruktura, z której prowadzone są testy, oraz miejsce przetwarzania wyników muszą znajdować się na terytorium Polski, czy wystarczy, że znajdują się na terytorium EOG.

Odpowiedź na pytanie nr 11:
Na potrzeby realizacji zamówienia infrastruktura wykorzystywana do prowadzenia testów oraz przetwarzania ich wyników może znajdować się zarówno na terytorium Polski, jak i innych państw Europejskiego Obszaru Gospodarczego (EOG). Lokalizacje te traktowane są równoważnie.

Wykonawca zobowiązany jest do wskazania lokalizacji infrastruktury testowej, miejsc przetwarzania informacji oraz państw, z których możliwy będzie dostęp do tych informacji, zgodnie z pkt 12 ust. 3 OPZ.

Przetwarzanie informacji niepublicznych GIOŚ lub dostęp do nich spoza EOG wymaga uprzedniej, wyraźnej zgody Zamawiającego oraz spełnienia pozostałych warunków określonych w OPZ i Umowie.

W celu usunięcia wątpliwości interpretacyjnych Zamawiający nadaje § 15 ust. 3 PPU następujące brzmienie:
„3. Infrastruktura wykorzystywana do prowadzenia testów bezpieczeństwa oraz przetwarzania informacji, wyników testów i materiałów dowodowych może znajdować się na terytorium Polski lub innego państwa Europejskiego Obszaru Gospodarczego (EOG). Wykonawca zobowiązany jest do uprzedniego ujawnienia Zamawiającemu lokalizacji tej infrastruktury oraz państw, z których możliwy jest dostęp do informacji Zamawiającego. Przetwarzanie informacji niepublicznych Zamawiającego lub dostęp do nich spoza EOG wymaga uprzedniej, wyraźnej zgody Zamawiającego, udokumentowanej oceny ryzyka oraz spełnienia wymagań określonych w OPZ, Umowie i obowiązujących przepisach prawa."

Pozostałe wymagania dotyczące ochrony informacji oraz zasad wykorzystywania narzędzi testowych, w tym wymagania pkt 12 ust. 2–5 OPZ, pozostają bez zmian.

Pytanie nr 12:

Pytanie – rozbieżność dotycząca kryterium oceny ofert Pkt 6 zapytania ofertowego wspomina o „deklaracji składanej na potrzeby kryterium oceny ofert" w zakresie miejsca przetwarzania informacji GIOŚ, a pkt 12 ust. 3 OPZ – o „przyznaniu 0 punktów". Wśród kryteriów oceny ofert nie ma jednak kryterium dotyczącego lokalizacji przetwarzania. Prosimy o potwierdzenie, że ofertę ocenia się wyłącznie według kryteriów C, L i E, a deklaracja w tym zakresie nie jest wymagana.

Odpowiedź na pytanie nr 12:

Oferty będą oceniane wg kryteriów, o których mowa w pkt. 9 Zapytania ofertowego tj.:

1) *Cena brutto danej Części (C) – 60 pkt;*
2) *Liczba wykonanych testów bezpieczeństwa (L) – 20 pkt, odpowiednio:*
   a) *dla Części I (L-I) – liczba wykonanych testów infrastruktury IT i sieciowej;*
   b) *dla Części II (L-II) – liczba wykonanych testów serwisów WWW i API;*
3) *Kompetencje i doświadczenie eksperta wiodącego (E) – 20 pkt.*

Zamawiający wyjaśnia, że wspomniane w pytaniu sformułowania dotyczące deklaracji na potrzeby kryterium oceny ofert oraz „przyznania 0 punktów" nie ustanawiają dodatkowego kryterium oceny. Należy ją traktować jako oczywistą omyłkę pisarską. Oferty będą oceniane wyłącznie według kryteriów C, L i E oraz wag określonych w pkt 9 Zapytania ofertowego.

Lokalizacja infrastruktury oraz miejsca przetwarzania informacji nie stanowią odrębnego kryterium oceny ofert. Zamawiający nie wymaga składania odrębnej deklaracji w tym zakresie na etapie składania ofert.
Powyższe nie znosi obowiązku ujawnienia przez Wykonawcę lokalizacji przetwarzania informacji GIOŚ oraz państw, z których możliwy będzie dostęp do tych informacji, zgodnie z pkt 12 ust. 3 OPZ i § 15 ust. 2 PPU, przed rozpoczęciem realizacji testów.

Pytanie nr 13:

Szanowni Państwo, zwracamy się z uprzejmą prośbą o wydłużenie terminu składania ofert do dnia 20.11.2026 r. ze względu na przypadający w tym okresie długi weekend związany ze świętem 11 listopada oraz związany z nim wysoki sezon urlopowy. Z góry dziękujemy. Z poważaniem,

Departament Informatyzacji
Telefon: +48 22 577 51 70
e-mail: sekretariatdinf@gios.gov.pl
ul. Chmielna 132/134, 00-805 Warszawa
Główny Inspektorat Ochrony Środowiska

Odpowiedź na pytanie nr 13:
Nie przewiduje się wydłużenia terminu składania ofert do dnia 20 listopada 2026 r.

Decyzja ta wynika z konieczności zachowania harmonogramu realizacji zamówienia, w szczególności zakończenia testów bezpieczeństwa, przeprowadzenia procedur odbiorowych oraz rozliczenia projektu grantowego w wymaganych terminach.

W związku z powyższym termin składania ofert pozostaje bez zmian, tj. do dnia 13 listopada 2026 r. do godz. 9:00.

Wiktor Fediuszko
Zastępca Dyrektora
Główny Inspektorat Ochrony Środowiska
/ – podpisany elektronicznie/

Departament Informatyzacji
Telefon: +48 22 577 51 70
e-mail: sekretariatdinf@gios.gov.pl

ul. Chmielna 132/134, 00-805 Warszawa
Główny Inspektorat Ochrony Środowiska