



Główny Urząd Statystyczny
Departament Administracyjno-Budżetowy

Warszawa, dnia 14.07.2020 r.

Wyjaśnienia SIWZ

Działając na podstawie art. 38 ust. 1, 1a i 2 ustawy Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843 i z 2020 r. poz. 288), Zamawiający odpowiada na pytania do SIWZ zadane przez wykonawców w postępowaniu o udzielenie zamówienia pn.: „Kontraktowanie aktualizacji, weryfikacji oraz dostosowania dokumentów SZBI, wykonania przeglądów i audytu w ramach projektu „Wdrożenie Kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji – KSZBI dla statystyki publicznej” w ramach 2 Osi priorytetowej Programu Operacyjnego Polska Cyfrowa (POPC) na lata 2014-2020 współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego.”; numer sprawy: 28/ST/KSZBI/POPC/PN/2020, ogłoszenie o zamówieniu numer 2020/S 121-296469 z dnia 25-06-2020 r.

Pytanie 6:

Dotyczy Załącznik nr 1 do SIWZ, str. 1, l., 5., 3), „Dokumenty SZBI dla poszczególnych systemów teleinformatycznych/procesów.” Ile jest systemów teleinformatycznych/procesów? Ewentualnie prosimy o oszacowanie objętości tej dokumentacji z dokładnością do 100 stron.

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że nie jest znana dokładna ilość dokumentów SZBI, z uwagi na fakt, że obecnie trwają prace nad wprowadzaniem, aktualizacją dokumentacji SZBI w jssp. Przyjmuje się jednak, że łącznie we wszystkich jssp będzie nie mniej niż 4000 stron dokumentacji SZBI. Ponadto Zamawiający wyjaśnia, że w jednostkach służb statystyki publicznej nie obowiązuje obecnie jeden szablon dokumentów SZBI. W Polityce Bezpieczeństwa Informacji Statystyki Publicznej przyjęto, że Prezes GUS zatwierdza polityki w zakresie bezpieczeństwa informacji, dyrektorzy jednostek zatwierdzają dokumenty SZBI obowiązujące wyłącznie w danej jednostce, natomiast Pełnomocnik SZBI zatwierdza pozostałe dokumenty SZBI (inne niż Polityki i zatwierdzone przez Dyrektorów jednostek dokumenty) obowiązujące w statystyce publicznej. Konieczne jest zweryfikowanie, w ramach realizacji przedmiotu zamówienia, posiadanej dokumentacji i wydanie rekomendacji w przypadku stwierdzonych niezgodności i braków, które będą stanowiły podstawę do aktualizacji, dostosowania lub przygotowania dokumentacji SZBI. Liczba systemów na przedmiotowych wyjaśnieniach wynosi 183 sztuki. Systemy mają zróżnicowany poziom złożoności technicznej i liczbę użytkowników od 1 do kilku tysięcy. Podana liczba zawiera też systemy do obsługi infrastruktury i narzędziowe.

Pytanie 7:

Dotyczy Załącznik nr 1 do SIWZ, str. 4, IV, 1., 2), b) i c) i d). Prosimy o wyjaśnienie stwierdzenia „obserwacje on-line audytora”, w szczególności, czy oznacza to wizje lokalne, czy pozyskiwanie informacji w trybie zdalnym?

Odpowiedź Zamawiającego:

Zamawiający informuje, że w dniu 10.07.2020 r. upublicznił modyfikację SIWZ, zmieniającą zapisy Załącznika nr 1 do SIWZ (OPZ) w zakresie pkt. IV./1./2. Zgodnie z powyższą modyfikacją sformułowanie „obserwacje on-line audytora” zmienione zostały na:

- obserwacje lub wywiady zdalne audytora, dotyczące bezpieczeństwa fizycznego i środowiskowego (GUS i CIS z siedzibą w Warszawie, Zakład CIS w Radomiu),

- obserwacje lub wywiady zdalne audytora, dotyczące bezpieczeństwa serwerowni GUS zarządzanych przez CIS (lokalizacja Warszawa i Radom),
- obserwacje lub wywiady zdalne audytora dotyczące bezpieczeństwa 4 kluczowych systemów teleinformatycznych statystyki publicznej i wskazanych przez Zamawiającego pozostałych 8 systemów statystyki publicznej.

W zapisach tych przewidziane są obserwacje na miejscu lub wywiady zdalne audytora, gdzie wywiady zdalne rozumiane są jako pozyskiwanie informacji w trybie zdalnym. Zdalnie Zamawiający udostępni wyłącznie dokumenty jawne.

Pytanie 8:

Dotyczy Załącznik nr 1 do SIWZ, str. 4, IV, 1., 2) d). Czy dobrze rozumiemy, że obserwacje on-line audytora dotyczące bezpieczeństwa 4 kluczowych systemów teleinformatycznych statystyki publicznej i wskazanych przez Zamawiającego pozostałych 8 systemów statystyki publicznej są rozumiane jako analiza dokumentacji bezpieczeństwa związanej z tymi systemami i ewentualne, ogólne zweryfikowanie architektury systemu bezpieczeństwa, bez praktycznego sprawdzania skuteczności jego wdrożenia, w szczególności bez testów penetracyjnych i weryfikacji konfiguracji urządzeń?

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że obserwacje lub wywiady zdalne audytora rozumiane jako analiza dokumentacji bezpieczeństwa związanej z tymi systemami, weryfikację rzeczywistego stosowania zapisów dokumentacji SZBI i ogólne zweryfikowanie architektury systemu bezpieczeństwa, bez praktycznego sprawdzania skuteczności jego wdrożenia, w szczególności bez testów penetracyjnych i weryfikacji konfiguracji urządzeń. Przedmiotem zamówienia nie jest przeprowadzenie testów penetracyjnych. Zdalnie Zamawiający udostępni wyłącznie dokumenty jawne.

Pytanie 9:

Dotyczy Załącznik nr 1 do SIWZ, str. 4, IV, 1., 4). Czy w zapisie tym 50% dotyczy jedynie dokumentacji, czy również analizy środowiska i zasobów teleinformatycznych?

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że przeprowadzony audyt „zerowy” uwzględniać będzie weryfikację na dzień audytu co najmniej 50% dokumentacji SZBI. Wskazana minimalna próba badania audytowego w wymiarze 50% nie dotyczy analizy środowiska i zasobów teleinformatycznych.

Pytanie 10:

Dotyczy Załącznik nr 1 do SIWZ, str. 4, IV, 1., 4). Czy określenie „Przeprowadzony audyt „zerowy” uwzględniać będzie weryfikację (...) zasobów teleinformatycznych (m.in. badanie ich stosowania)” oznacza weryfikację faktu praktycznego zastosowania zidentyfikowanych zasobów teleinformatycznych? Chcemy się upewnić, że nie ma być to weryfikacja skuteczności wdrożenia i jakości działania, np. w oparciu o sprawdzenia CIS Benchmark.

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że określenie „przeprowadzony audyt „zerowy” uwzględniać będzie weryfikację (...) zasobów teleinformatycznych (m.in. badanie ich stosowania)” oznacza weryfikację zgodności stosowanych zabezpieczeń z zapisami dokumentacji SZBI. Nie dotyczy to weryfikacji w oparciu o CIS Benchmark.

Pytanie 11:

Dotyczy Załącznik nr 1 do SIWZ, str. 5, IV., 1., 7), a. O jakie certyfikacje chodzi w zapisie „wymagań niezbędnych do certyfikacji;”

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że zapisy pkt IV.1.7) Załącznika nr 1 do SIWZ, odnoszą się chodzi o certyfikacji ISO/IEC 27001.

Pytanie 12:

Dotyczy Załącznik nr 1 do SIWZ, str. 8, IV., 2., 11) i 12) i 14). Czy uogólnienie zapisów dotyczących zakresu prac do postaci „bezpieczeństwa informacji”, bez odniesienia do kwestii dokumentacji oznacza, że należy wykonać audyt zastosowanych rozwiązań technicznych, w tym urządzeń teleinformatycznych (zapór sieciowych, systemów AAA, AV,

ochrony poczty elektronicznej i innych rozwiązań bezpieczeństwa), ich wzajemnych powiązań, zastosowania itd? Tak sugeruje zapis „... z uwzględnieniem środków aktualnie wykorzystywanych przez Zamawiającego”. Zwracamy uwagę, że audyt techniczny/technologiczny w przypadku GUS jest zadaniem bardzo złożonym i znacząco zwiększy pracochłonność.

Odpowiedź Zamawiającego:

Zamawiający wyjaśnia, że uogólnienie zapisów pkt IV.2.11), 12) i 14) Opisu przedmiotu zamówienia, nie oznacza że należy wykonać audyt zastosowanych rozwiązań technicznych, w tym urządzeń teleinformatycznych (zapór sieciowych, systemów AAA, AV, ochrony poczty elektronicznej i innych rozwiązań bezpieczeństwa), ich wzajemnych powiązań, zastosowania. Przedmiotem zamówienia jest wykonanie audytu diagnostycznego „zerowego” jako element rozpoznania spełniania przez Zamawiającego wymagań organizacyjno-technicznych, prawnych, zgodności z normami ISO oraz opracowania założeń do Systemu Zarządzania Bezpieczeństwem Informacji oraz aktualizacja, weryfikacja i odpowiednio dostosowanie lub opracowanie dokumentów Systemu Zarządzania Bezpieczeństwem Informacji, w tym realizacja rekomendacji z przeprowadzonego audytu „zerowego” oraz przeprowadzenie przeglądów SZBI. W ramach audytu Wykonawca przeprowadza weryfikację zgodności stosowanych zabezpieczeń z zapisami dokumentacji SZBI a także weryfikację pod kątem optymalizacji stosowanych zabezpieczeń i w ramach realizacji zadania II opracuje listę środków technicznych niezbędnych dla zapewnienia bezpieczeństwa informacji z uwzględnieniem środków aktualnie wykorzystywanych przez Zamawiającego. Z uwagi na fakt, że Zamawiający w okresie świadczenia usługi przez Wykonawcę przewiduje rozbudowę infrastruktury teleinformatycznej statystyki publicznej, Wykonawca aktualizując lub odpowiednio opracowując dokumentację SZBI (Zadanie nr II) uwzględni zachodzące zmiany.

Pytanie 13:

Dotyczy Załącznik nr 7 do SIWZ, str. 8, § 3, 6), d). Czy możemy prosić o wskazanie wymagań bezpieczeństwa informacji wynikających ze współpracy międzynarodowej Statystyki publicznej, jakie mają być uwzględnione w przedmiotowym projekcie?

Odpowiedź Zamawiającego:

Zasady bezpieczeństwa informacji w Europejskim Systemie Statystycznym określone zostały w dokumencie „ESS IT Security Framework”, który oparty jest 100% o normy ISO:IEC 27001 i 27002.

Przewodnicząca
Komisji Przetargowej
Agnieszka Jagoda
Konsultant
w Wydziale zamówień Publicznych GUS