Nr sprawy: 35/D/23

Załącznik nr 2b do SWZ

Dostawa oprogramowania podnoszącego poziom cyberbezpieczeństwa systemów teleinformatycznych oraz usługę audytu bezpieczeństwa systemów IT w ramach środków pochodzących z Funduszu Przeciwdziałania COVID-19 - podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców dla potrzeb SP ZOZ MSWiA w Łodzi

Wymagania dotyczące audytu bezpieczeństwa

Audyt bezpieczeństwa, o którym mowa może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w poniższym wykazie certyfikatów uprawiających do przeprowadzenia audytu lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

Wykaz certyfikatów uprawniających do przeprowadzenia audytu:

a) Certified Internal Auditor (CIA);

b) Certified Information System Auditor (CISA);

c) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

d) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;

e) Certified Information Security Manager (CISM);

f) Certified in Risk and Information Systems Control (CRISC);

g) Certified in the Governance of Enterprise IT (CGEIT);

h) Certified Information Systems Security Professional (CISSP);

i) Systems Security Certified Practitioner (SSCP);

j) Certified Reliability Professional;

k) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności (wdrożeniu zakupionych w niniejszym postępowaniu rozwiązań czyberbezpieczeństwa) , oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.

Terminy:

Zamawiający wymaga przeprowadzenia audytu oraz dostarczenia raportu kończącego audyt w terminie do 21 Listopada 2023r

Oferta musi zawierać dokładny opis działań wchodzących w skład audytu oraz potwierdzenie posiadania niezbędnych uprawnień do przeprowadzenia audytu.