Ogólne informacje o zamówieniu na

**Badanie potrzeb małych i średnich przedsiębiorstw z branży cyberbezpieczeństwa**

do przeprowadzenia Wstępnych konsultacji rynkowych

**Część I.** Główne założenia oraz cele Badania potrzeb małych i średnich przedsiębiorstw z branży cyberbezpieczeństwa (dalej zwanego Badaniem).

Badanie zostanie zrealizowane w ramach projektu finansowanego z Programu Cyfrowa Europa.

Zamówienie ma na celu przedstawienie wyników badania małych i średnich przedsiębiorców z branży cyberbezpieczeństwa, w zakresie ich potencjału, potrzeb i barier rozwojowych, a następnie przygotowanie raportu badawczego uwzględniającego rekomendacje w zakresie rozwoju branży cyberbezpieczeństwa w Polsce.

Badanie powinno pozwolić na zdiagnozowanie potencjalnych obszarów wsparcia małych i średnich przedsiębiorców z branży cyberbezpieczeństwa w celu wzmocnienia potencjału krajowego w tej branży oraz na zidentyfikowanie podmiotów mogących stać się członkami Społeczności kompetentnej, o której mowa w art. 8 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiającego Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji.

Zamówienie składa się z 4 części:

1. mapowanie branży cyberbezpieczeństwa, w zakresie małych i średnich przedsiębiorców wraz z opisem aktualnego potencjału tej branży;
2. analiza barier i potrzeb małych i średnich przedsiębiorców z branży cyrerbezpieczeństwa;
3. identyfikacja małych i średnich przedsiębiorców mających potencjał merytoryczny (identyfikacja będzie dotyczyć tylko tego aspektu, z wyłączeniem innych kryteriów rekrutacyjnych do Społeczności kompetentnej) do kandydowania na członka Społeczności kompetentnej, zgodnie z art. 8 ww. rozporządzenia;
4. raportu z badania uwzględniającego rekomendacje służące rozwojowi małych i średnich przedsiębiorców z branży cyberbezpieczeństwa oraz wzrostowi ich konkurencyjności na rynku międzynarodowym.

**Część II.** Zagadnienia wspomagające szacowanie wartości zamówienia.

Etapy realizacji:

1. Wstępny.

Wykonanie właściwego badania rynku małych i średnich przedsiębiorców musi zostać poprzedzone przygotowaniem metodologii, jaka zostanie zastosowania do określenia populacji oraz jej segmentów. Badaniem mają zostać objęte przedsiębiorstwa, które są wytwórcami produktów i usług z obszaru cyberbezpieczeństwa, rozumianego zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r. poz.913 ze zm.). Na potrzeby badania ta ogólna definicja powinna ulec doprecyzowaniu, pozwalając na określenie czy dana działalność i jej intensywność pozwala na uznanie, że podmiot prowadzi działalność w tej branży, czy jest to działanie okazjonalne lub uzupełniające. Stworzenie mapy branży cyberbezpieczeństwa będzie zatem wymagało między innymi dokonania jej opisu poprzez segmenty/specjalizacje/potencjał technologiczny[[1]](#footnote-1), które powinny być zdefiniowane przez Wykonawcę z uwzględnieniem istniejących opracowań zaadoptowanych do warunków krajowych. Wybór taksonomii lub stworzenie własnej powinien być przez wykonawcę uzasadniony. Dodatkowo opis branży mśp cyberbezpieczeństwa będzie wymagał uwzględnienia m.in. rozkładu terytorialnego, analizy wielkości przedsiębiorców, zasobów itp.

Zamawiający chce badaniem objąć całą populację lub próbę w zależności od efektów tego etapu prac. Ponadto podczas niniejszego etapu powinny zostać zdiagnozowane źródła danych, w tym kontaktowych do małych i średnich przedsiębiorstwach z branży cyberbezpieczeństwa.

1. Przygotowania narzędzia i strategii badania

Na tym etapie Wykonawca w uzgodnieniu z Zamawiającym przygotuje szczegółowe cele badawcze i narzędzia służące ich osiągnięciu, w tym formularz/ankietę badawczą. Wskaże adekwatne do celów badania i jego zakresu techniki badawcze. Badanie powinno odpowiadać na takie pytania jak:

1. Jak wygląda branża mśp cyberbezpieczeństwa w Polsce:
	1. Jakiej wielkości podmioty działają na rynku krajowym?
	2. Czy są to podmioty krajowe (kapitał pochodzi z Polski)? Czy filie/oddziały firm zagranicznych/spółki powiązane, z siedzibą w PL?
	3. W jakim obszarze [specjalizacji technologicznej] cyberbezpieczeństwa działają?
	4. Jaki długo działają?
	5. W jakich województwach mają swoją siedzibę?
	6. Jaki jest zasięg terytorialny ich działania – krajowy/międzynarodowy?
	7. Czy należą do stowarzyszeń branżowych, klastrów, izb przemysłowych lub innych organizacji reprezentujących interesy branży, a jeśli tak to do których?
2. Jakim potencjałem dysponują mśp branży cyberbezpieczeństwa?
	1. Liczba zatrudnionych pracowników?
	2. Potencjał merytoryczny kadry, rozumiany jako kluczowe umiejętności zgodnie z European Cybersecurity Skills Framework oraz posiadane wykształcenie i certyfikaty specjalistyczne?
	3. Potencjał technologiczny (mapa kompetencji technologicznych – w jakich podmiotach, w których województwach jak się one przedstawiają).
	4. Posiadane patenty, certyfikacje?
	5. Roczne dochody (w przedziałach)?
	6. Udział w rynku?
3. Perspektywy rozwojowe dla branży cyberbezpieczeństwa ?
	1. Czy przedsiębiorcy w najbliższym roku swojej działalności planują nowe inwestycje, w szczególności w infrastrukturę R+B?
	2. Czy przedsiębiorcy planują rozszerzenie swojej działalności np. terytorialnie – krajowo/międzynarodowo lub też co do oferty?
	3. Jeśli nie planują rozszerzyć swojej działalności to dlaczego (np. brak wiedzy, brak inwestora)?
	4. Czy wprowadzenie CRA i NIS 2 wpłynie na działalność przedsiębiorstwa? W jaki sposób?
	5. Czy są plany dotyczące certyfikacji produktów?
	6. Czy w podmiocie jest wiedza w temacie certyfikacji produktów/usług?
	7. Jakie zdaniem przedsiębiorców obszary cyberbezpieczeństwa będą mieć największy potencjał rozwojowy w najbliższych latach?
4. Bariery i ograniczenia dla rozwoju branży.
	1. Jakie bariery i ograniczenia widzą przedsiębiorcy w rozwoju swojej działalności obecnie?
	2. Jaki problemy branża może mieć w przyszłości?
	3. Czy bariery te zależą od wielkości przedsiębiorstwa, jego siedziby, specjalizacji itp.?
5. Pokonanie barier i ograniczeń.
6. Czy bariery te mogą być pokonane na szczeblu przedsiębiorców i rynku czy potrzebna jest interwencja państwa?
7. Jeśli tak to jaka interwencja państwa jest potrzebna i jak intensywna powinna być, a może państwo powinno się z jakichś działań/interwencji wycofać?
8. Jakie inicjatywy państwa są oceniane jako wspierające rozwój branży cyberbezpieczeństwa w kraju?
9. Czy granty publiczne (dotacje dla przedsiębiorców) ułatwiłyby rozwój branży cyberbezpieczeństwa w kraju?
10. Jeśli tak to na jakie działania powinny być przeznaczone i jaka powinna być ich wysokość?
11. Jakie inne działania mogłyby wpłynąć pozytywnie na krajową branże cyberbezpieczeństwa (np. zwolnienia podatkowe, ułatwienia w dostępie do zamówień publicznych)?
12. Czy znane są przedsiębiorcom programy unijne dające możliwość rozwoju produktu/usługi i jej wdrożenie np. Horyzont Europa, Cyfrowa Europa, FENG i inne?
13. Czy przedsiębiorcy korzystali do tej pory ze wsparcia finansowego krajowego i z UE w celu wsparcia rozwoju ( w szczególności na projekty R+B) oraz działań dot. ekspansji firmy?
14. Jeśli tak, z jakich programów i jaka była kwota realizowanego projektu i finansowania/współfinansowania krajowego/UE?
15. Społeczność kompetentna
16. Które z badanych podmiotów dysponują potencjałem, który mógłby zostać wykorzystany w działaniach Społeczności kompetentnej [informacje o Społeczności kompetentnej na stronie [www.gov.pl/web/cyber-nccpl](http://www.gov.pl/web/cyber-nccpl).

Ankieterzy powinni mieć zapewnione materiały pomocnicze oraz zostać przeszkoleni adekwatnie do celów badania i stosowanych technik badawczych.

3. Przygotowanie bazy danych i raportu z badania

Raport z badania powinien zawierać opis metodologii badania, mapę branży cyberbezpieczeństwa w kraju w obszarze małych i średnich przedsiębiorstw, wyniki badania, rekomendacje. Od Wykonawcy oczekuje się atrakcyjniej edytorsko formy dokumentu – w postaci elektronicznej w wersji polskiej i angielskiej.

Wykonawca przygotuje strukturę bazy danych oraz opis sposobu wprowadzania danych i kodowania badania ankietowego. Dodatkowo utworzy bazę danych mśp z branży cyberbezpieczeństwa zidentyfikowanych prze Wykonawcę podczas Badania. Zaproponuje rozwiązania techniczne umożliwiające Zamawiającemu korzystanie z baz danych za pomocą outsourcingowych narządzi.

1. Oczekiwania po przeprowadzonych konsultacjach rynkowych:

Uzyskanie informacji, które mają służyć Zamawiającemu do przygotowania opisu przedmiotu zamówienia, specyfikacji warunków zamówienia, oszacowania wartości zamówienia lub określenia warunków umowy w sprawie zamówienia a w szczególności do:

1. przygotowania w planowanym zakresie i kształcie badania;
2. określenia metodyki wyodrębnienia populacji objętej badaniem oraz próby badawczej;
3. określenia źródeł danych do badania i sposobów ich pozyskania;
4. określenia metody, technik przeprowadzenia badania;
5. określenia etapów prowadzenia badania;
6. wskazania sposobu prezentacji wyników i utworzenia bazy danych z badania;
7. określenia wymagań zamawiającego wobec Wykonawców;
8. określenia kosztów całkowitych takiego badania oraz czasu potrzebnego na przeprowadzenie badania i napisanie raportu;
9. określenia personelu i kwalifikacji personelu niezbędnego do przygotowania i przeprowadzenia takiego badania.

Dodatkowe dokumentu do wykorzystania:

1. ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 poz. 913 ze zm.);
2. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. ustanawiającego Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa [dalej zwane ECCC] oraz sieć krajowych ośrodków koordynacji;
3. opracowanie PARP pn. Mapa rozwoju rynku i technologii dla obszaru cyberbezpieczeństwa (<https://smart.gov.pl/pl/analizy-i-raporty>);
4. Cybersecurity taxonomy (<https://op.europa.eu/en/web/eu-vocabularies/concept-scheme/-/resource?uri=http://data.jrc.ec.europa.eu/ontology/cybersecurity/cybersecurity-taxonomy>)
5. European Cybersecurity Skills Framework <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>

1. Przykładowa taksonomia w zakresie cyberbezpieczeństwa https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy [↑](#footnote-ref-1)