KARTA OCENY PROJEKTU NR P310 PRZEZ ZESPÓŁ ZADANIOWY RADA ARCHITEKTURY IT	
NAZWA PROJEKTU: „Podłączenie podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem S46 (S46-react)"	
WNIOSKODAWCA: Minister Cyfryzacji	
BENEFICJENT: Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy	
DATA DOKUMENTU: 22.07.2021 (wpływ do RA)	
PRZEBIEG OCENY:	**1.** Przesłanie członkom RA IT w dniu 4.08.2021 r. drogą mailową „Opisu założeń projektu informatycznego" do zapoznania się i zgłaszania uwag. **2.** Sformułowanie uwag RA i uzyskanie wyjaśnień od wnioskodawcy. **3.** Ocena opisu założeń na posiedzeniu w dniu 25.08.2021 i podjęcie rekomendacji.
REKOMENDACJA:	☐ POZYTYWNA ☒ **POZYTYWNA Z ZALECENIEM WPROWADZENIA W NIM ZMIAN I UZUPEŁNIEŃ NA DALSZYM ETAPIE PRAC NAD PROJEKTEM** ☐ NEGATYWNA ☐ KONIECZNOŚĆ PONOWNEGO ZAOPINIOWANIA PO SPEŁNIENIU OKREŚLONYCH WYMOGÓW LUB W INNYM TERMINIE
UWAGI ARCHITEKTÓW:	☒ **TAK** ☐ NIE
UWAGI:	Rada architektury IT zaleca: 1. Rozdział 1.1: Identyfikacja problemu i potrzeb: - Wskazano liczby interesariuszy: *„Jednostki samorządu terytorialnego i jednostki im podległe (Urzędy Marszałkowskie, JST zarządzające większymi miastami, spółki wodno-kanalizacyjne itp.), urzędy współpracujące przy zagadnieniach związanych z cyberbezpieczeństwem JST, a także uczestniczące w zintegrowanym systemie zarządzania kryzysowego (Urzędy Wojewódzkie, RCB), większe szpitale" – 100* *„Przedstawiciele JST i jednostek im podległych, urzędów współpracujące przy zagadnieniach związanych z cyberbezpieczeństwem JST, a także uczestniczących w zintegrowanym systemie zarządzania kryzysowego (Urzędy Wojewódzkie, RCB)" - 200* **Uwaga:** należy rozważyć zmianę zapisów w Kamieniach milowych (rozdział 3), bowiem przy zapisach „narastających" można łatwo wywieść, że zarówno grupa jednostek jak i przedstawicieli będzie znacznie większa (przewyższająca podaną w rozdziale 1.1.), czyli 230 – jednostek i 460 – przedstawicieli. Jednocześnie należy zwrócić uwagę na doprecyzowanie interesariuszy projektu zgodnie z art. 4 ustawy o KSC. Określenie grupy docelowej projektu na poziomie min. 100 JST.

	- Zapis: *"niewystarczający poziom wiedzy pracowników jednostek organizacyjnych samorządów terytorialnych oraz innych – wskazanych podmiotów o cyberbezpieczeństwie"* **Uwaga:** W projekcie zaplanowano tylko szkolenie z zakresu wykorzystania systemu oraz jako wskaźnik podaje się podniesienie kompetencji cyfrowych podczas gdy w zidentyfikowanych problemach jest mowa o niewystarczającym poziomie wiedzy pracowników JST. Wydaje się, że przeszkolenie z wykorzystania systemu jest zatem niewystarczającą odpowiedzią na tak zidentyfikowany problem 2. Rozdział 1.2: Opis stanu obecnego – W pierwszym akapicie wskazano jako cel systemu m.in.: *„zapewniającego **obserwację** ryzyka na poziomie krajowym"*, **Uwaga**: Zgodnie z ustawą KSC system ma zapewnić **szacowanie** ryzyka na poziomie krajowym - sformułowanie "obserwacja" jest niewystarczające. 3. Rozdział 2.1: Cele i korzyści wynikające z projektu – W podsumowaniu Celu 1 wpisano: *„Zwiększenie liczby podłączeń do systemu S46 wraz z przeszkoleniem użytkowników i tym samym wzrost poziomu cyberbezpieczeństwa RP, wpisuje się bezpośrednio w zakres osiągnięcia wyżej wymienionych celów strategicznych."* **Uwaga:** Brak informacji w ustawie o możliwości korzystania z system przez JST – mowa jest, że CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej mogą korzystać z systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji. W porozumieniu określa się zakres i warunki korzystania z systemu teleinformatycznego. W związku z powyższym wydaje się, że może być konieczna zmiana ustawy lub należy podać odpowiednią inną formalną podstawę precyzyjnie określającą role i relacje KSC v. JST. 4. Rozdział 5.1: Ryzyka wpływające na realizację projektu – Dla ryzyka „Wzrost kursu" wskazano sposób zarządzania ryzykiem: *„Przeniesienie – realizacja postępowań zakupowych odpowiednio wcześnie i z odpowiednim budżetem, tak aby dodatkowe ryzyko przenieść na Wykonawcę."* **Uwaga:** Wskazany sposób zarządzania ryzykiem bardziej pasuje do kategorii „Mitygacja", a nie „Przeniesienie".
	5. Rozdział 5.2: Ryzyka wpływające na utrzymanie efektów – Dla ryzyka *„Brak chęci do użytkowania systemu S46 przez podłączone podmioty"* wskazano sposoby zarządzania ryzykiem jako: Akceptacja – podejmowanie działań zaradczych na bieżąco i Przeniesienie – zaangażowanie innych podmiotów w uświadamianie roli systemu S46 **Uwaga**: Należy uszczegółowić na czym mają polegać działania zaradcze oraz o jakie inne podmioty chodzi oraz wskazania w jaki sposób ma to działanie wpłynąć na podniesienie chęci użytkowania

	systemem. Przyjęta zasada dobrowolności udziału JST sprowadza niekontrolowane zagrożenie dla powodzenia projektu 6. Rozdział 8: Otoczenie prawne – Zgodnie z zapisem Ustawa o Krajowym Systemie Cyberbezpieczeństwa (t. j. Dz. U. 2020 poz. 1369) nie wymaga zmiany **Uwaga:** Brak informacji w ustawie o możliwości korzystania z system przez JST – mowa jest, że CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej mogą korzystać z systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji. W porozumieniu określa się zakres i warunki korzystania z systemu teleinformatycznego. W związku z powyższym wydaje się, że może być konieczna zmiana ustawy lub jak w uwadze 2.1 należy podać odpowiednią inną podstawę formalną precyzyjnie określającą role i relacje KSC v. JST . – Dla celu 2: *„Zwiększenie liczby podmiotów krajowego systemu cyberbezpieczeństwa posiadających umiejętność posługiwania się systemem S46."* Sformułowano KPI: *„Liczba pracowników objętych szkoleniami w zakresie umiejętności cyfrowych."* **Uwaga:** W projekcie zaplanowano tylko szkolenie z zakresu wykorzystania systemu oraz jako wskaźnik podaje się podniesienie kompetencji cyfrowych podczas gdy w zidentyfikowanych problemach jest mowa o niewystarczającym poziomie wiedzy pracowników JST. Wydaje się, że przeszkolenie z wykorzystania systemu jest zatem niewystarczająca odpowiedzią na zidentyfikowany problem. Być może KPI powinno być inaczej zdefiniowane.

Zastępca Kierownika Zespołu

Andrzej Ręgowski