

Warszawa, 16 maja 2024 r.

ZZPR.51.1.2024

**Sz. P. Marcin Wysocki**  
**Zastępca Dyrektora**  
**Departament Cyberbezpieczeństwa**  
**Ministerstwo Cyfryzacji**  
**ul. Królewska 27**  
**00-060 Warszawa**

Dotyczy: opisu założeń projektu informatycznego S46 finansowanego w ramach KPO

Szanowny Panie Dyrektorze,

W załączeniu przekazuję skorygowany opis założeń projektu informatycznego pn. „Podłączenie 385 nowych podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem (system S46) oraz dalszy rozwój tego systemu” (wersje xml, pdf). Projekt jest realizowany w ramach programu: Krajowy Plan Odbudowy i Zwiększania Odporności, inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo.

Załączam listę modyfikacji wyjaśnień do uwag omawianych w trakcie posiedzenia KRMC w dniu 13 maja 2024 roku. Załączam również kolejną wersję opisu założeń projektu.

Zwracam się z prośbą o przekazanie jej do Komitetu Rady Ministrów do spraw Cyfryzacji.

Z poważaniem  
Dyrektor Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego  
Radosław Nielek

Załącznik nr 1: Zebrana lista odpowiedzi na uwagi wprowadzonych zmian

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
1	GUS	2.1. Cele i korzyści wynikające z projektu, Cel – 3, Korzyść	Brak informacji o kosztach podłączenia podmiotu krajowego systemu cyberbezpieczeństwa do Systemu S46.	Po treści:  „(...) c) Udostępnienie mechanizmów komunikacji dostosowanych do potrzeb podmiotów kluczowych i ważnych;”  <b>Dodać zapis</b> dot. kosztów ponoszonych przez podmioty krajowego systemu cyberbezpieczeństwa	<b>Uwzględniono:</b> zaproponowano zapis o redukcji kosztów a nie eliminacji, ponieważ koszty po stronie uczestnika będą sprowadzać się do zapewnienia personelu obsługującego system oraz stanowisk pracy dla nich. Zakłada się, że mechanizmy komunikacji, o których mowa w projekcie, nie będą wymagać ponoszenia dodatkowych kosztów.  <b>Zmiany:</b> dodanie zapisu w rozdz. 2.1 cel 3, korzyściach.  d) redukcja kosztów korzystania z usług systemu S46 po stronie podmiotów kluczowych i ważnych;
2.	MON	1.1. Identyfikacja problemu i potrzeb	Zapis dotyczący zwiększania odporności systemu S46 ma wspierać realizację określonych zadań wynikających z UKSC. Zadania te wiążą się z zapewnieniem cyberbezpieczeństwa, a te rozumiane jako działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami. W tym kontekście odwołanie do zapewnienia odporności na działania naruszające bezpieczeństwo jest zbyt szerokie.	(...) jest jednym z podstawowych i istotnych zagadnień zwiększających holistycznie odporności systemów informacyjnych RP na cyberzagrożenia	Uwzględniono.  Zmiany: w rozdz. 1.1 „identyfikacja problemów i potrzeb” zmieniono wskazany akapit zgodnie z propozycją:  (...) jest jednym z podstawowych i istotnych zagadnień zwiększających holistycznie odporności systemów informacyjnych RP na cyberzagrożenia

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
3	MON	1.1. Identyfikacja problemu i potrzeb	Mając na uwadze informacje w OSR dotyczące procedowanego projektu Ustawy zmieniającej do ustawy o krajowym systemie cyberbezpieczeństwa (dalej: projekt nowelizacji UoKSC) wątpliwości budzą szacowane wielkości grupy w tabeli dotyczącej je z informacjami w OSR	Brak	<b>Uwzględniono:</b> uspojniono licznosci grup interesariuszy z OSR projektu nowelizacji UoKSC.  <b>Zmiany:</b>  Interesariusz nr 3; szacowana wielkość grupy: <b>38147</b>
4	MON	2.1. Cele i korzyści wynikające z projektu	Odnośnie KPI – należy rozważyć weryfikację wartości docelowych, przy uwzględnieniu informacji zawartych w OSR do projektu ustawy zmieniającej UKSC	Brak.	<b>Wyjaśnienie:</b> Wskaźniki nie uległy zmianie, ponieważ wskaźnik 385 podmiotów został notyfikowany. Wskaźnik ten został wskazany jako minimalny. Modernizacja S46 ma na celu przygotowanie systemu do większej obsługi większej liczby podmiotów. Wielkość grupy oszacowano poprzez sumowanie odpowiednich pozycji OSR, dotyczących podmiotów kluczowych i ważnych. Odjęto od tej liczby 385 podmiotów będących aktualnymi OUK.  <b>Zmiany:</b> brak

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
5	MON	2.2 udostępnione e-Uslugi	<p>Odnosnie wskazanych e-usług należy uwzględnić też usługę wpisywanie podmiotów kluczowych lub podmiotów ważnych do wykazu z urzędu przez ministra właściwego do spraw informatyzacji, jak i przez inne organy właściwe do spraw cyberbezpieczeństwa (zgodnie z projektem ustawy zmieniającej uksc).</p> <p>Odnosnie usługi wymiany wiadomości należy uwzględnić nie tylko ich wymianę pomiędzy podmiotami kluczowymi i ważnymi, ale też innymi podmiotami KSC.</p>	<p>W opisie e-usługi samorejestracji, po wyrażeniu „Ze strony organów właściwych możliwe będzie obsługa wniosków o wpis” dodać „oraz wpisywanie podmiotów kluczowych lub podmiotów ważnych do wykazu z urzędu przez ministra właściwego do spraw informatyzacji i organy właściwe do spraw cyberbezpieczeństwa”.</p> <p>W opisie usługi wymiany wiadomości, po wyrażeniu „pomiędzy podmiotami kluczowymi i ważnymi” dodać „oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa”, a wyrażenie „dostosowana do potrzeb podmiotów kluczowych i ważnych wymiana wiadomości” zmienić na „dostosowana do potrzeb podmiotów krajowego systemu cyberbezpieczeństwa wymiana wiadomości”</p>	<p><b>Uwzględniono:</b></p> <p><b>Zmiany:</b> w rozdziale 2.2 nazwa usługi:</p> <p>Usługa 1: po wyrażeniu „Ze strony organów właściwych możliwe będzie obsługa wniosków o wpis” dodano „oraz wpisywanie podmiotów kluczowych lub podmiotów ważnych do wykazu z urzędu przez ministra właściwego do spraw informatyzacji i organy właściwe do spraw cyberbezpieczeństwa”.</p> <p>Usługa 2: W opisie usługi wymiany wiadomości, po wyrażeniu „pomiędzy podmiotami kluczowymi i ważnymi” dodano „oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa”, a wyrażenie „dostosowana do potrzeb podmiotów kluczowych i ważnych wymiana wiadomości” zmieniono na „dostosowana do potrzeb podmiotów krajowego systemu cyberbezpieczeństwa wymiana wiadomości”</p>
6	MON	6. otoczenie prawne	Odnosnie Ustawy o Krajowym Systemie Cyberbezpieczeństwa zaktualizować informacje, projektu ustawy zmieniającej	W kolumnie etap prac legislacyjnych – zastąpić wyrażenie „uzgodnienia wewnętrzne” wyrażeniem „opiniowanie”	<p><b>Wyjaśnienie:</b> Formularz umożliwia wybranie predefiniowanych wartości pośród których nie ma wartości „opiniowanie”. Dopuszczalne wartości to:</p> <ul style="list-style-type: none"> <li>• Uzgodnienia wewnętrzne</li> <li>• Uzgodnienia międzyresortowe</li> <li>• Komitet Rady Ministrów do Spraw Cyfryzacji;</li> <li>• Komitet do spraw Europejskich</li> <li>• Stały Komitet Rady Ministrów;</li> <li>• Komisja Prawnicza</li> </ul>

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
					<ul style="list-style-type: none"> <li>• Rada Ministrów</li> <li>• Sejm</li> <li>• Senat</li> </ul> <p><b>Zmiany:</b> zmieniono wartość na „uzgodnienia międzyresortowe”</p>
7	MON	7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu	W obecnie procedowanym projekcie ustawy zmieniającej uksc informacje o wykazie są ujęte w art. 7 ust. 2 (a nie art. 7 ust. 3) – zakres informacji nieco się różni, w projekcie ustawy jest dodatkowo ujęta informacja o numerze w wykazie i dacie wpisu do wykazu, a deklaracja podmiotu odnosi się do kryteriów mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy (a nie dużego, średniego, małego lub mikroprzedsiębiorcy)	<p>Zgodnie z propozycją nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa:</p> <p>„Art. 7.2. Wykaz, o którym mowa w ust. 1, zawiera:</p> <ol style="list-style-type: none"> <li>1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego;</li> <li>2) sektor, podsektor i rodzaj podmiotu, zgodnie z załącznikiem nr 1 lub nr 2 do ustawy;</li> <li>3) siedzibę i adres do korespondencji;</li> <li>4) adres do doręczeń elektronicznych, jeżeli został nadany;</li> <li>5) adres poczty elektronicznej;</li> <li>6) numer identyfikacji podatkowej (NIP), jeżeli został nadany;</li> <li>7) numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON);</li> <li>8) numer we właściwym rejestrze działalności</li> </ol>	<p><b>Wyjaśnienie:</b> skorygowano numerację. Ze względu na <b>ograniczenie liczby liter</b> w polu formularza, jest możliwe wstawienie pełnego tekstu zawartości wykazu.</p> <p><b>Zmiany:</b></p> <p>Zmieniono wartość pola na:</p> <p>Zgodnie z propozycją nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa:</p> <p>„Art. 7.2. Wykaz, o którym mowa w ust. 1, zawiera:</p> <ol style="list-style-type: none"> <li>1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego;</li> <li>2) sektor, podsektor i rodzaj podmiotu, zgodnie z załącznikiem nr 1 lub nr 2 do ustawy;</li> <li>3) siedzibę i adres do korespondencji;</li> <li>4) adres do doręczeń elektronicznych, jeżeli został nadany;</li> <li>5) adres poczty elektronicznej;</li> <li>6) numer identyfikacji podatkowej (NIP), jeżeli został nadany;</li> </ol>

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
				<p>regulowanej, jeżeli został nadany;</p> <p>9) zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny;</p> <p>10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny;</p> <p>11) dane, co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej;</p> <p>12) numer telefonu przyporządkowany do wykonywanej działalności;</p> <p>13) deklarację podmiotu kluczowego lub podmiotu ważnego czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy;</p> <p>14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność wraz z określeniem wykonywanej działalności;</p> <p>15) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierające nazwę (firmę) dostawcy, siedzibę, adres, numer telefonu, adres poczty</p>	<p>7) numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON);</p> <p>8) numer we właściwym rejestrze działalności regulowanej, jeżeli został nadany;</p> <p>9) zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny;</p> <p>10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny;</p> <p>11) dane, co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej;</p> <p>12) numer telefonu przyporządkowany do wykonywanej działalności;</p> <p>13) deklarację podmiotu kluczowego lub podmiotu ważnego czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy;</p> <p>14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność wraz z określeniem wykonywanej działalności;</p> <p>15) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierające nazwę (firmę) dostawcy, siedzibę,</p>

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
				<p>elektronicznej;</p> <p>16) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego, o którym mowa w art. 5 ust. 4, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące:</p> <p>a) w przypadku osób fizycznych: imię i nazwisko, adres, numer telefonu oraz adres poczty elektronicznej,</p> <p>b) w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej: nazwę (firmę) przedstawiciela, siedzibę, adres, numer telefonu, adres poczty elektronicznej;</p> <p>17) informację o zawarciu przez podmiot kluczowy lub podmiot ważny porozumienia, o którym mowa w art. 8h ust. 5;</p> <p>18) informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny;</p> <p>19) wskazanie organu właściwego do spraw cyberbezpieczeństwa właściwy dla podmiotu kluczowego lub podmiotu ważnego;</p> <p>20) wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu ważnego;</p> <p>21) wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu</p>	<p>adres, numer telefonu, adres poczty elektronicznej;</p> <p>16) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego, o którym mowa w art. 5 ust. 4, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące:</p> <p>a) w przypadku osób fizycznych: imię i nazwisko, adres, numer telefonu oraz adres poczty elektronicznej, [...]"</p>

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
				kluczowego lub podmiotu ważnego;  22) numer w wykazie;  23) datę wpisu do wykazu;  24) tytuł prawny wpisania do wykazu, o którym mowa w ust. 1;  25) datę wykreślenia z wykazu, o którym mowa w ust. 1.”	
8	MON	7.5 Bezpieczeństwo	Należy rozważyć dostosowanie systemu do wymagań aktualnej normy WCAG 2.1 (zgodnie z ustawą z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych), a przed udostępnieniem usługi dokonać oceny dostępności cyfrowej oraz przygotować deklarację dostępności.	Po zdaniu „Dokumentacja projektowa systemu została opracowana zgodnie z Web Content Accessibility Guidelines (WCAG 2.0) i przyjęta przez MC.” dodać:  „System zostanie dostosowany do wymagań WCAG 2.1., a przed udostępnieniem zostanie dokonana ocena dostępności cyfrowej oraz opracowana deklaracja dostępności.”	<b>Uwzględniono:</b> Pierwotnie, w trakcie zgłaszania projektu jako jednego z projektów finansowanych ze środków KPO, planowano realizację połączeń w modelu izolowanym od sieci publicznej. Włączenie usługi rejestracji podmiotów kluczowych i ważnych, wraz ze zmianą modelu udostępnienia za pośrednictwem sieci Internet i narzędzi takich jak Węzeł Krajowy, spowodowało, że konieczne jest wprowadzenie zmiany w przedmiotowym punkcie.  <b>Zmiana:</b>  Zmiana wyboru na: „system podlega rygorom KRI”. Zmiana skutkuje usunięciem dodatkowego opisu w Rozdziale 7.5



Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
9	MON	7.5 Bezpieczeństwo	<p>Należy zweryfikować informację czy system rzeczywiście nie podlega rygorom <i>rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI)</i>.</p> <p>Zgodnie z opisem „Projektowanie i eksploatacja systemu odbywa się z uwzględnieniem Polskich Norm dotyczących bezpieczeństwa (w szczególności PN-EN ISO/IEC 27001) „, a zgodnie z rozporządzeniem KRI wymagania określone w rozporządzeniu uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń; PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do</p>		<p><b>Uwzględniono:</b> Pierwotnie, w trakcie zgłaszania projektu jako jednego z projektów finansowanych ze środków KPO, planowano realizację połączeń w modelu izolowanym od sieci publicznej. Włączenie usługi rejestracji podmiotów kluczowych i ważnych, wraz ze zmianą modelu udostępnienia za pośrednictwem sieci Internet i narzędzi takich jak Węzeł Krajowy, spowodowało, że konieczne jest wprowadzenie zmiany w przedmiotowym punkcie.</p> <p><b>Zmiana:</b></p> <p>Zmiana wyboru na: „system podlega rygorom KRI”. Zmiana skutkuje usunięciem dodatkowego opisu w Rozdziale 7.5</p>

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
			odtworzenia techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.		
10	Ministerstwo Rozwoju	Uwaga ogólna	Pytanie: czy S46 będzie obsługiwał SSO (Single Sign-On) z portalami takimi jak biznes.gov.pl	n.d.	<b>Wyjaśnienie:</b> W ramach realizacji projektu planuje się integrację z Węzłem Krajowym. Tam gdzie będzie to możliwe, będzie zastosowany mechanizm SSO.
11	MSWiA	Źródło finansowania	<p>W opisie w zakresie źródeł finansowania projektu wskazano m.in. „... budżet państwa, część budżetowa - w trakcie ustaleń”.</p> <p>Uprzejmie proszę o informację na jakim etapie przewidują Państwo dookreślenie tej kwestii i czy zakładają Państwo wskazanie tu części budżetowych, których dysponentem jest Minister SWiA (cz. 17, 42, 43)</p>	n.d.	<p><b>Wyjaśnienie:</b> Finansowanie z budżetu państwa dotyczy wartości podatku VAT (~2mln zł). Wartość podatku VAT nie jest kosztem kwalifikowanym KPO. Wartość „w trakcie ustaleń” została wprowadzona ze względu na to, że jest ustalane kompleksowe podejście do finansowania VAT, w projektach korzystających ze środków KPO.</p> <p>Nie przewiduje się wykorzystywania części budżetowych Ministra SWiA.</p>