Nazwa dokumentu: Opis założeń projektu informatycznego - Podłączenie 385 nowych podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem (system S46) oraz dalszy rozwój tego systemu.					
Lp.	**Organ wnoszący uwagi**	**Jednostka redakcyjna, do której wnoszone są uwagi**	**Treść uwagi**	**Propozycja zmian zapisu**	**Odniesienie do uwagi**
1	MON	1.1. Identyfikacja problemu i potrzeb	Zapis dotyczący zwiększania odporności systemu System S46 ma wspierać realizację określonych zadań wynikających z uksc. Zadania te wiążą się z zapewnieniem cyberbezpieczeństwa, a te jest 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 wewnętrzne i zewnętrzne jest zbyt szerokie.	(…) jest jednym z podstawowych i istotnych zagadnień zwiększających holistycznie odporności systemów informacyjnych RP na cyberzagrożenia.	
2	MON	1.1. Identyfikacja problemu i potrzeb	Mając na uwadze informacje w OSR dot. procedowanego projektu ustawy zmieniającej do ustawy o krajowym systemie cyberbezpieczeństwa wątpliwości budzą szacowane wielkości grupy w tabeli dotyczącej zidentyfikowanych problemów. Należy zweryfikować je z informacjami w OSR.		
3	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.		
4	MON	2.2. Udostępnione e-usługi	Odnośnie wskazanych e-usług należy uwzględnić tez 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). Odnośnie usługi wymiany wiadomości należy uwzględnić nie tylko ich wymianę pomiędzy	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”. W opisie usługi wymiany wiadomości, po wyrażeniu „pomiędzy podmiotami kluczowymi i ważnymi” dodać	

			podmiotami kluczowymi i ważnymi, ale też innymi podmiotami KSC.	„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"	
5	MON	6. Otoczenie prawne	Odnośnie Ustawy o Krajowym Systemie Cyberbezpieczeństwa – należy zaktualizować informacje, projekt ustawy zmieniającej jest na etapie opiniowania.	W kolumnie etap plac legislacyjnych - zastąpić wyrażenie „uzgodnienia wewnętrzne" wyrażeniem „opiniowanie".	
6	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)	Zgodnie z propozycją nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa: „Art. 7.2. Wykaz, o którym mowa w ust. 1, zawiera: 1) ·nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego; 2) ·sektor, podsektor i rodzaj podmiotu, zgodnie z załącznikiem nr 1 lub nr 2 do ustawy; 3) ·siedzibę i adres do korespondencji; 4) ·adres do doręczeń elektronicznych, jeżeli został nadany; 5) ·adres poczty elektronicznej; 6) ·numer identyfikacji podatkowej (NIP), jeżeli został nadany; 7) ·numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON); 8) ·numer we właściwym rejestrze działalności regulowanej, jeżeli został nadany; 9) ·zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny; 10) ·domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny; 11) ·dane, co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej; 12) ·numer telefonu przyporządkowany do wykonywanej	

				działalności; 13) ·deklarację podmiotu kluczowego lub podmiotu ważnego czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy; 14) ·informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność wraz z określeniem wykonywanej działalności; 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 elektronicznej; 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: a) ·w przypadku osób fizycznych: imię i nazwisko, adres, numer telefonu oraz adres poczty elektronicznej, b) ·w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej: nazwę (firmę) przedstawiciela, siedzibę, adres, numer telefonu, adres poczty elektronicznej; 17) ·informację o zawarciu przez podmiot kluczowy lubo podmiot ważny porozumienia, o którym mowa w art. 8h ust. 5; 18) ·informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny; 19) ·wskazanie organu właściwego do spraw cyberbezpieczeństwa właściwy dla podmiotu kluczowego lub podmiotu ważnego; 20) ·wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu ważnego; 21) ·wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu 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.”	
7	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.”	
8	MON	7.5 Bezpieczeństwo	Należy zweryfikować informację czy system rzeczywiście nie podlega rygorom *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). 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 odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.		