|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Nazwa dokumentu:***  **Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne** | | | | | |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
| **1** | **MAP** | Art. 1 pkt 31 | Proponuje się wprowadzenie przepisu doprecyzowującego zakres działania operatora sieci komunikacji strategicznej, w tym wskazujące zakres usług świadczonych przez operatora obowiązkowo.  W projektowanym art. 59zd proponuje się dodanie ust. 3, który wymienia obligatoryjne zadania operatora sieci komunikacji strategicznej, w tym zadania realizowane dla MON, MSWiA oraz MSZ, a także budowę Bezprzewodowej Sieci Łączności Specjalnej | 3. Operator sieci komunikacji strategicznej świadczy usługi:   1. dla Ministra Obrony Narodowej w zakresie: 2. utrzymania, rozbudowy i modyfikacji sieci teleinformatycznej na potrzeby obsługi Sił Zbrojnych RP, 3. zestawienia i utrzymania łączy dostępowych do sieci, o której mowa w lit. a; 4. dla ministra właściwego do spraw wewnętrznych w zakresie: 5. utrzymania, rozbudowy i modyfikacji sieci teleinformatycznej na potrzeby obsługi numerów alarmowych, 6. zestawienia i utrzymania łączy dostępowych do sieci, o której mowa w lit. a dla:  * użytkowników centralnej ewidencji pojazdów i centralnej ewidencji kierowców, * jednostek Państwowej Straży Pożarnej, * dyspozytorni Państwowego Ratownictwa Medycznego i Lotniczego Pogotowia Ratunkowego, * Centrum Personalizacji Dokumentów, * Zakładu Emerytalno-Rentowego Ministerstwa Spraw Wewnętrznych,  1. utrzymania i rozbudowy sieci teleinformatycznej na potrzeby rejestru mieszkańców, rejestru zamieszkania cudzoziemców i rejestru stanu cywilnego; 2. utrzymania i rozbudowy sieci teleinformatycznej GOVNET; 3. utrzymania i rozbudowy sieci teleinformatycznej na potrzeby rejestru PESEL; 4. zapewnienia połączenia centrów powiadamiania ratunkowego z publiczną siecią telekomunikacyjną 5. dla ministra właściwego do spraw zagranicznych w zakresie: 6. świadczenia usług telekomunikacyjnych w systemie łączności satelitarnej, 7. świadczenia usług sieci rozległej WAN; 8. budowy i utrzymania Bezprzewodowej Sieci Łączności Specjalnej, o której mowa w art. 59ze. | **Uwaga nieuwzględniona**  Katalog usług, który będzie świadczył operator sieci komunikacji strategicznej nie powinien być ustalony w ustawie – będzie to niepotrzebnie zawężało możliwości świadczenia usług przez tego operatora. |
| **2** | **MAP** | Art. 1 pkt 31 | W konsekwencji uwagi nr 1, Art. 59zd ust. 3 zostaje oznaczony jako ust. 4, a odesłanie w nim zawarte odsyła do ust. 5 tego artykułu. | 1. Operator sieci komunikacji strategicznej świadczy usługi telekomunikacyjne w celu realizacji zadań, o których mowa w ust. 1, oraz może świadczyć inne usługi w zakresie realizacji tych zadań, jeżeli podmioty, o których mowa w ust. 5, zgłoszą operatorowi sieci komunikacji strategicznej wniosek o ich realizację, i spełniony jest jeden z następujących warunków:   1) w związku z ich realizacją konieczne jest nadanie związanej z nimi dokumentacji klauzuli, zgodnie z przepisami o ochronie informacji niejawnych, lub  2) wymaga tego istotny interes bezpieczeństwa państwa, ze szczególnym uwzględnieniem cyberbezpieczeństwa państwa, lub  3) wymaga tego ochrona bezpieczeństwa publicznego, lub  4) muszą im towarzyszyć szczególne środki bezpieczeństwa. | **Uwaga nieuwzględniona**  Uzasadnienie jak w uwadze nr 1. |
| **3** | **MAP** | Art. 1 pkt 31 | W konsekwencji uwagi nr 1, Art. 59zd ust. 4 zostaje oznaczony jako ust. 5, a dotychczasowy ust. 5 oznacza się jako ust. 6.  Proponuje się dodanie ust. 7 dotyczącego możliwości zlecenia operatorowi sieci komunikacji strategicznej usług wsparcia technicznego przy realizacji zadań ustawowych wymienionych w proponowanym przepisie służb. | 1. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne oraz Komenda Główna Policji mogą zlecić operatorowi sieci komunikacji strategicznej świadczenie usługi wsparcia technicznego przy realizacji ich zadań ustawowych. | **Uwaga nieuwzględniona**  Uzasadnienie jak w uwadze nr 1. |
| **4** | **MAP** | Art. 1 pkt 31 | Wydaje się zasadne jawne wprowadzenie w projektowanych przepisach kwestii powołania i działania Bezprzewodowej Sieci Łączności Specjalnej. Proponuje się w projektowanym art. 59ze, ust. 1 oznaczyć jako ust. 2 i dodać ust. 1, zawierający definicję Bezprzewodowej Sieci Łączności Specjalnej.  Proponowana zmiana treści ust. 2 doprecyzowuje, że częstotliwości przyznane operatorowi sieci komunikacji strategicznej będą służyć świadczeniu usługi Bezprzewodowej Sieci Łączności Specjalnej. | Art. 59ze. 1. Bezprzewodowa Sieć Łączności Specjalnej jest siecią w standardzie 5G lub wyższym, zapewniającą komunikację bezprzewodową i transmisję danych oraz usługi powiązane dla podmiotów, o których mowa w ust. 4, 5 i 6.  2. Operator sieci komunikacji strategicznej świadczy usługi Bezprzewodowej Sieci Łączności Specjalnej w oparciu o zasoby częstotliwości, o których mowa w art. 1154 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. | **Uwaga nieuwzględniona**  Nie jest konieczne regulowanie w ustawie nazwy „*Bezprzewodowej Sieci Łączności Specjalnej”.* Każdorazowa zmiana nazwy będzie musiała się dokonywać w drodze ustawy. Ponadto występuje trudność w skonstruowaniu definicji legalnej standardu 5G. |
| **5** | **MAP** | Art. 1 pkt 31 | Proponuje się wprowadzenie przepisu, który jednoznacznie potwierdzi odpłatny charakter usług operatora sieci komunikacji strategicznej i zwolnienie przy powierzaniu tych usług z ustawy Prawo zamówień publicznych. W tym celu proponuje się dodanie art. 59zg, który stanowi, że do umów zawieranych przez podmioty do tego upoważnione z operatorem sieci komunikacji strategicznej nie stosuje się przepisów ustawy – Prawo zamówień publicznych a cena usług objętych tymi umowami powinna być ustalona z uwzględnieniem zasad handlowych i interesu publicznego. | Art. 59zg. 1. Przy zawieraniu umów dotyczących realizacji zadań, o których mowa w art. 59zd i art. 59ze, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2019 r. poz. 2019 i z 2020 r. poz. 288, 1517 oraz 2320).  2.  Cena za usługi świadczone przez operatora sieci komunikacji strategicznej ustalana jest z uwzględnieniem zasad handlowych i interesu publicznego. | **Uwaga nieuwzględniona**  Kwestia ceny za usługi świadczone przez operatora sieci komunikacji strategicznej powinna być ustalona w umowie między tym operatorem a podmiotem korzystającym z jego usług. |
| **6** | **MAP** | Art. 2 | W celu zapewnienia zgodności z projektowanym przepisem art. 59ze ustawy o Krajowym Systemie Cyberbezpieczeństwa, w projektowanym art. 1154 w ust. 1 proponuje się zmianę wyrażenia „może zapewnić” na „zapewnia”. Dotychczasowa redakcja przepisu nie zapewnienia częstotliwości operatorowi sieci komunikacji strategicznej.  Proponuje się również w ust. 2 dodanie pkt 7, który wyraźnie określi, że Prezes UKE w analizie powinien uwzględnić także zapewnienie realizacji zadań operatora sieci komunikacji strategicznej.  Proponuje się uzupełnienie regulacji określonej w ust. 5 o obowiązek zapewnienia przez Prezesa UKE częstotliwości dla operatora sieci łączności strategicznej na potrzeby Bezprzewodowej Sieci Łączności Specjalnej w decyzji rezerwacyjnej. Proponuje się także dodanie ust. 6 i ust. 7, które wprost określają możliwość by podmiotem wskazanym na mocy ust. 4 mógł być w szczególności operator sieci komunikacji strategicznej, jak również, by podmiot wskazany na mocy ust. 4 mógł, za zgodą prezesa UKE, powołać osobę prawną, która świadczyła by usługi udostępniania pojemności sieci na zasadach hurtowych. Podmiot wskazany przez Prezesa Rady Ministrów na mocy ust. 4 powinien zachować większościowe udziały oraz być przedsiębiorcą dominującym w rozumieniu art. 4 pkt 3 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2019 r. poz. 369, 1571 i 1667) w takiej osobie prawnej. | Art. 1154. 1. Prezes UKE zapewnia odpowiednie częstotliwości w celu oferowania przez przedsiębiorcę telekomunikacyjnego na zasadach niedyskryminacyjnych usług na warunkach hurtowych w celu ich dalszej sprzedaży przez innego przedsiębiorcę telekomunikacyjnego.  2. Zapewnienie częstotliwości, o którym mowa w ust. 1, poprzedza analiza Prezesa UKE, która uwzględnia:   1. stopień realizacji celów wynikających z dokumentów programowych Unii Europejskiej na terytorium Rzeczypospolitej, w tym w szczególności w zakresie pokrycia terytorium kraju infrastrukturą zapewniającą dostęp do sieci bardzo szybkich przepustowości; 2. możliwości efektywnego wykorzystania częstotliwości; 3. stan rynku telekomunikacyjnego; 4. plany inwestycyjne przedsiębiorców telekomunikacyjnych; 5. długoterminowe spodziewane korzyści społeczno-gospodarcze; 6. promowanie innowacyjnych usług cyfrowych. 7. zapewnienie realizacji zadań operatora sieci komunikacji strategicznej, o których mowa w Rozdziale 11b ustawy o Krajowym Systemie Cyberbezpieczeństwa.   3. Wyniki analizy, o której mowa w ust. 3, Prezes UKE przedstawia Prezesowi Rady Ministrów w terminie 30 dni od dnia jej sporządzenia.  4. Prezes Rady Ministrów, w oparciu o analizę, o której mowa w ust. 3, w celu zapewnienia realizacji celów wynikających z dokumentów programowych Unii Europejskiej, w szczególności w zakresie pokrycia terytorium kraju infrastrukturą zapewniającą dostęp do sieci bardzo szybkich przepustowości, może wyznaczyć podmiot, który świadczył będzie usługi, o których mowa w ust. 1.  5. Podmiot, o którym mowa w ust. 4, wykorzystuje częstotliwości do wykonywania zadań, o których mowa w ust. 1, na podstawie decyzji o rezerwacji częstotliwości wydanej przez Prezesa UKE po uzgodnieniu z ministrem właściwym do spraw informatyzacji. Prezes UKE zapewnia w decyzji rezerwacyjnej częstotliwość na potrzeby świadczenia usług Bezprzewodowej Sieci Łączności Specjalnej, o której mowa w art. 59ze ustawy o Krajowym Systemie Cyberbezpieczeństwa.  6. Przedsiębiorcą telekomunikacyjnym o którym mowa w ust 4 może być w szczególności operator sieci komunikacji strategicznej, który przydzieloną częstotliwość w pierwszej kolejności wykorzystuje w celu realizacji zadań wskazanych w ustawie o Krajowym Systemie Cyberbezpieczeństwa, a w pozostałym zakresie oferuje na zasadach określonych w ust. 1  7. Prezes UKE może wyrazić zgodę na powołanie przez przedsiębiorcę telekomunikacyjnego, o którym mowa w ust. 4 osoby prawnej, której celem ma być świadczenie usług udostępniania pojemności sieci na zasadach hurtowych i określić warunki funkcjonowania takiej osoby prawnej, mając na uwadze, że większościowe udziały w takiej osobie prawnej oraz pozycję dominującą w rozumieniu art. 4 pkt 3 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz.U. z 2019 r. poz. 369, 1571 i 1667) musi zachować przedsiębiorca telekomunikacyjny, o którym mowa w ust. 4.”. | **Uwaga nieuwzględniona**  Kompetencja Prezesa UKE, z której będzie korzystać stosownie do okoliczności, powinna pozostać fakultatywna. |
| **7** | **MAP** | Art. 3 | Po art. 2 proponuje się dodanie art. 3 i odpowiednią zmianę numeracji kolejnych artykułów. Proponowany przepis ma na celu zmianę w ustawie z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw w celu stworzenie możliwości pokrycia zasięgiem Bezprzewodowej Sieci Łączności Specjalnej obszaru całej Polski, w tym tzw. „białych plam”.  Przedsiębiorca telekomunikacyjny, o którym mowa w art. 59zd ust. 2 ustawy o Krajowym Systemie Cyberbezpieczeństwa powinien być uprawniony do bezpłatnego umieszczania na nieruchomościach należących do Skarbu Państwa, Lasów Państwowych, państwowych osób prawnych, jednostek samorządu terytorialnego oraz państwowych lub samorządowych jednostek organizacyjnych, obiektów i urządzeń infrastruktury telekomunikacyjnej.  Przyjęcie takiego rozwiązania obniży też koszty funkcjonowania Bezprzewodowej Sieci Łączności Specjalnej. | Art. 3. W ustawie z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz.U. poz.1815) po art. 17 dodaje się art. 17a w brzmieniu:  "Art. 17a. Przedsiębiorca telekomunikacyjny, o którym mowa w art. 59zd ust. 2 ustawy o Krajowym Systemie Cyberbezpieczeństwa jest uprawniony do bezpłatnego umieszczania na nieruchomościach należących do Skarbu Państwa, Lasów Państwowych, państwowych osób prawnych, jednostek samorządu terytorialnego oraz państwowych lub samorządowych jednostek organizacyjnych, obiektów i urządzeń infrastruktury telekomunikacyjnej, w szczególności instalowania urządzeń telekomunikacyjnych, przeprowadzania linii kablowych pod nieruchomością, na niej lub nad nią, umieszczanie tabliczek informacyjnych o urządzeniach, a także ich eksploatacji i konserwacji, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia wartości nieruchomości.". | **Uwaga nieuwzględniona**  Kwestia zmian legislacyjnych *w ustawie o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw* powinna być przedmiotem odrębnej ustawy. Uwzględnienie jej w przedmiotowym projekcie wymagałaby także zmiany wpisu do wykazu. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
| **1** | **MZ** | Załącznik nr 1 do ustawy  kolumna „Rodzaj podmiotów” dotycząca Sektora „Ochrona zdrowia” | Ograniczenie liczby potencjalnych operatorów usług kluczowych oraz dostosowanie do najważniejszych i najbardziej kluczowych podmiotów w sektorze ochrony zdrowia.  Na skutek obecnie przyjętych przepisów w sektorze ochrony zdrowia zidentyfikowano około 230 podmiotów. Jest to więcej niż suma wszystkich zidentyfikowanych podmiotów w innych sektorach. Obowiązujące obecnie przepisy uniemożliwiają włączenie do krajowego systemu cyberbezpieczeństwa niektórych, najważniejszych podmiotów w sektorze ochrony zdrowia. W związku z powyższym, konieczne jest dostosowanie podmiotów wskazanych w załączniku do ustawy do najważniejszych i najbardziej kluczowych podmiotów w sektorze ochrony zdrowia.  Podmioty lecznicze, w przedsiębiorstwie których funkcjonują dział farmacji szpitalnej lub apteka szpitalna są faktycznie tożsame z podmiotami leczniczymi, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. Brak jest jakiegokolwiek uzasadnienia dla istnienia wyodrębnienia takich podmiotów, ponieważ podmioty posiadające dział farmacji lub aptekę szpitalną są podmiotami leczniczymi, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. | a) skreśla się „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2020 r. poz. 944).”  b) skreśla się „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.” | **Uwaga uwzględniona**  Dodatkowo chcemy podkreślić, że jako podmioty publiczne zostaną dodane do KSC samodzielne publiczne zakłady zdrowotne (np. pogotowie ratunkowe, wojewódzkie szpitale zespolone). Zmiana jest podyktowana szczególnym znaczeniem świadczonych zadań publicznych na rzecz obywateli. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
| **1** | **MI** | art. 5 ust. 4 Ustawy o Krajowym Systemie Cyberbezpieczeństwa | Podtrzymanie pierwotnie zgłoszonej uwagi. Przedstawione uzasadnienie do nieuwzględnienia uwagi nie odnosi się do istotnego problemu, jakim jest wyznaczenie jednego podmiotu na OUK przez Polskę i inne Państwo członkowskie UE.  W nawiązaniu do art. 5 ust. 4 „W przypadku gdy podmiot świadczy usługę kluczową w innych państwach członkowskich Unii Europejskiej, organ właściwy do spraw cyberbezpieczeństwa w toku postępowania administracyjnego, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzi konsultacje z tymi państwami w celu ustalenia, czy ten podmiot został uznany w tych państwach za operatora usługi kluczowej oraz w kontekście stwierdzenia, że „Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej – art. 5 ust. 1 zgłasza się następujący problem: Z konsultacji z Pojedynczym Punktem Kontaktowym nie wynikają żadne decyzje. Ustawa nie wskazuje, jak należy postąpić wobec operatorów usług kluczowych posiadających na terenie Rzeczypospolitej Polskiej oddział będący w rozumieniu ustawy jednostką organizacyjną, a jednocześnie wyznaczonych w innym kraju UE na operatora.  Brak takiej regulacji istotnie utrudnia podjęcie właściwej decyzji o wyznaczeniu podmiotu na operatora usługi kluczowej (zwanego dalej OUK) oraz ma negatywny wpływ na ocenę sposobu postępowania w realizacji zadań wynikających  z Ustawy o Krajowym Systemie Cyberbezpieczeństwa, zarówno ze strony OUK, jak i organu właściwego. | Ustawa powinna określić, czy organ właściwy ds. cyberbezpieczeństwa powinien również wyznaczyć tego operatora na terenie Rzeczypospolitej Polskiej oraz w jakim przypadku:   * jeżeli system informacyjny operatora wykorzystywany do świadczenia usługi kluczowej jest posadowiony i administrowany na terytorium Rzeczypospolitej Polskiej, * jeżeli system informacyjny wykorzystywany do świadczenia usługi kluczowej nie jest posadowiony i administrowany na terytorium Rzeczypospolitej Polskiej, * innym, niż w/w. | **Uwaga nieuwzględniona**  Ustawa o krajowym systemie cyberbezpieczeństwie w art. 5 ust. 4 wdrożyła art. 5 ust. 4 dyrektywy 2016/1148 NIS wraz z motywem 24 dyrektywy.  Zgodnie z tymi przepisami organ właściwy ds. cyberbezpieczeństwa może za pomocą Pojedynczego Punktu Kontaktowego konsultować się z organami właściwymi w innych państwach UE w kwestii wyznaczenia podmiotu za operatora usługi kluczowej, jeżeli już w innym państwie świadczy usługę kluczową. Konsultacje te mają pomóc organom właściwym różnym państw UE *w ocenie krytycznego charakteru danego operatora, jeżeli chodzi o wpływ transgraniczny, umożliwiając tym samym każdemu z zaangażowanych państw członkowskich przedstawienie swoich uwag dotyczących ryzyk związanych ze świadczonymi usługami.* (motyw 24 Dyrektywy NIS).  W obecnym stanie prawnym nie ma przeszkód, aby ten sam podmiot był wyznaczony w 2 krajach UE jako operator usługi kluczowej.  Kwestia ta może zostać poruszona w pracach nad projektem dyrektywy NIS2. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
| **1** | **MSWiA** | Art. 1 pkt 31 w zakresie projektowanego rozdz. 11b (art. 59zd-59zf) | We wskazanym przepisie w ustawie o krajowym systemie cyberbezpieczeństwa dodaje się m.in. rozdział 11b „Operator sieci komunikacji strategicznej”.  Zakres tematyczny projektowanych regulacji wykracza poza ramy przedmiotowe ustawy o krajowym systemie cyberbezpieczeństwa.  Poza tym regulacje zawarte w projektowanym rozdziale 11b dotyczą zadań przypisanych obecnie Ministrowi Spraw Wewnętrznych i Administracji, który pełni obecnie faktyczną rolę operatora Sieci Łączności Rządowej. | Prośba o wyjaśnienia. | **Wyjaśnienie**  Przepisy dotyczące operatora sieci komunikacji strategicznej mają zapewnić bezpieczną łączność rządową za pomocą nowoczesnych technologii w tym także za pomocą systemów teleinformatycznych.  Operator sieci komunikacji strategicznej będzie zapewniał wyższy poziom cyberbezpieczeństwa (w szczególności wyższej dostępności) usług świadczonych dla administracji rządowej. Nie będzie on świadczył usług komercyjnych.  Dlatego zasadne jest umieszczenie tych przepisów w ustawie o krajowym systemie cyberbezpieczeństwa. |
| **2** | **MSWiA** | Art. 1 pkt 31 w zakresie projektowanego rozdz. 11b (art. 59zd-59zf) | We wskazanym przepisie w ustawie o krajowym systemie cyberbezpieczeństwa dodaje się m.in. rozdział 11b „Operator sieci komunikacji strategicznej”. | Prośba o wyjaśnienie jak projektowane regulacje mają się do prac Międzyresortowego Zespołu ds. budowy i wdrożenia Sieci Komunikacji Rządowej. | **Wyjaśnienie**  Są to dwa różne projekty. To jest operator, który będzie zapewniał usługi infrastrukturalne, m.in. wykorzystywane m.in. przez Sieci Łączności Rządowej. |
| **3** | **MSWiA** | Art. 1 pkt 31 w zakresie projektowanego art. 59zd ust. 3 | Zgodnie z projektowanym przepisem „operator sieci komunikacji strategicznej świadczy **usługi** telekomunikacyjne w celu realizacji zadań, o których mowa w ust. 1, oraz może świadczyć **inne usługi** w zakresie realizacji tych zadań,...”.  Nie wskazano o jakie usługi chodzi. | Określenie usług jakie będzie świadczył operator sieci komunikacji strategicznej. | **Uwaga nieuwzględniona**  Katalog usług, który będzie świadczył operator sieci komunikacji strategicznej nie powinien być ustalony w ustawie – będzie to niepotrzebnie zawężało możliwości świadczenia usług przez tego operatora. |
| **4** | **MSWiA** | OSR, pkt 6, wiersz:  Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń | Wskazuje się na „powstanie operatora sieci komunikacji rządowej”. Sformułowanie to zostało użyte w tym miejscu, jak wynika z kontekstu, jako synonim sformułowania  „operator sieci komunikacji strategicznej”. | Prośba o wyjaśnienie czy „operator sieci komunikacji strategicznej” ma być faktycznie „operatorem sieci komunikacji rządowej” | **Wyjaśnienie**  OSR zostanie poprawiony, prawidłowa nazwa tego operatora to „operator sieci komunikacji strategicznej”. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
|  | **RCL** | Definicje | Projektowana definicja „cyberzagrożenia” (art. 1 pkt 2 lit f projektu ustawy zmieniającej) wymaga uzupełnienia, gdyż w wersji przekazanej w przedstawionym projekcie jej druga cześć jest trudna do odczytania. (…) „w inny sposób niekorzystnie wpłynąć w przypadku systemów informacyjnych, użytkowników takich systemów oraz innych osób;” Nie wiadomo na co może niekorzystnie wpłynąć cyberzagrożenie i do przypadku jakich systemów informacyjnych się odnosi. | Uzupełnienie definicji, zgodnie z merytoryczną decyzją projektodawcy | **Uwaga uwzględniona**  Przepis zostanie poprawiony:  „17) cyberzagrożenie – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na systemy informacyjne, użytkowników takich systemów oraz innych osób;”, |
|  | **RCL** | Upoważnienia ustawowe | W nowym projekcie ustawy są dokonywane zmiany w przepisach upoważaniających. Przykładowo dokonywana jest zmiana w art. 10 ust. 5 ustawy o KSC. Zgodnie z § 32 ust. 2 ZTP jeżeli zmiana dotyczy zakresu spraw przekazanych do uregulowania, rodzaju aktu lub wytycznych „przyjmuje się, że akt wykonawczy wydany na podstawie tego przepisu upoważniającego traci moc obowiązującą z dniem wejścia w życie przepisu zmieniającego treść przepisu upoważniającego.” W upoważnieniu z art. 10 ust. 5 pojęcie „cyberbezpieczeństwo” zostało zastąpione pojęciem „bezpieczeństwo systemów informacyjnych”. Będzie to powodowało zmianę sposobu określenia zakresu przedmiotowego aktu, co będzie skutkowało koniecznością modyfikacji tytułu oraz § 1 rozporządzenia. | Zasadnym wydaje się zastosowanie przepisu czasowo utrzymującego w mocy zgodnie z § 33 ZTP, w związku z dokonywanymi zmianami przepisów upoważniających. | **Uwaga uwzględniona**  Zostanie dodany przepis czasowo utrzymujący rozporządzenie. |
|  | **RCL** | Rozdział 5. Obowiązki podmiotu publicznego. Art. 21-25 ustawy o KSC | W zakresie art. 21-25 ustawy o KSC (art. 1 pkt 13-16 projektu ustawy zmieniającej) ponownej analizy wymaga katalog podmiotów objętych obowiązkami, kierowanymi do podmiotów publicznych. Weryfikacji wymaga odesłanie do art. 4 pkt 7-15 ustawy o KSC. Na skutek zmian w katalogu podmiotów objętych krajowym systemem cyberbezpieczeństwa (art. 4 ustawy o KSC), przy jednoczesnym zastosowaniu niezmienionego odesłania do art. 4 pkt 7-15 ustawy o KSC, jako taki podmiot publiczny klasyfikowany będzie również ISAC, o którym mowa w art. 4 pkt 7b ustawy o KSC. Ani ustawa ani uzasadnienie nie wskazują, że ISAC jest obligatoryjnie podmiotem o charakterze publicznym, który powinien być objęty obowiązkami, o których mowa w art. 21-25 ustawy o KSC. | Analiza odesłań do art. 4 ustawy o KSC w związku z projektowaną zmianą treści tego przepisu w zakresie katalogu podmiotów objętych obowiązkami, o których mowa w rozdziale 5 ustawy o KSC. | **Uwaga uwzględniona**  Przepis zostanie poprawiony. ISAC nie ma być podmiotem publicznym. |
|  | **RCL** | Art. 22 ustawy o KSC | Krajowym systemem cyberbezpieczeństwa są objęte również związki jednostek samorządu terytorialnego oraz związki metropolitalne (na mocy odesłania do art. 9 pkt 2 i 2a ustawy o finansach publicznych) oraz samorządowe zakłady budżetowe (odesłanie do art. 9 pkt 4 ustawy o finansach publicznych). Zmiana w art. 22 ustawy o KSC, wprowadzana projektem ustawy zmieniającej, zobowiązuje jednostki samorządu terytorialnego do przekazywania informacji o incydentach również wojewodzie. | Wymaga wyjaśnienia czy związki jednostek samorządu terytorialnego, związki metropolitalne czy samorządowe zakłady budżetowe będą również zobowiązane do zgłaszania incydentów wojewodzie czy też obowiązek ten będzie dotyczył jedynie jednostek samorządu terytorialnego. | **Wyjaśnienie**  Związki metropolitalne oraz związki jednostek samorządu terytorialnego, samorządowe zakłady budżetowe będą zgłaszać incydenty do wojewody, na terenie, którego wystąpił incydent. |
|  | **RCL** | Rozdział 5a. Zadania i obowiązki ISAC w ramach krajowego systemu cyberbezpieczeństwa | Ze względu na to, że wpis do wykazu ISAC nie warunkuje prowadzenia działalności jako ISAC ani umożliwia współpracy z podmiotami krajowego systemu cyberbezpieczeństwa funkcja wykazu ISAC prowadzonego przez ministra właściwego do spraw informatyzacji nie jest zrozumiała. W projektowanym kształcie może on stanowić bazę danych kontaktowych podmiotów gotowych do wykonywania zadań ISAC. Powstaje także wątpliwość czy mogą wykonywać zadania ISAC podmioty nie objęte wykazem i czy wykreślenie z wykazu, o którym mowa w art. 24a ust. 11 stanowi skuteczny środek zapobiegania naruszeniom przepisów i zasad współpracy w ramach krajowego systemu cyberbezpieczeństwa. | Przedstawienie wyjaśnienia i stosowna korekta przepisów po ich ponownej analizie. | **Wyjaśnienie**  Zadania ISAC w ramach krajowego systemu cyberbezpieczeństwa mają pełnić ISAC znajdujące się w wykazie.  ISAC będące w wykazie będą mogły być podłączone do systemu z art.. 46 KSC. |
|  | **RCL** | Art. 26 ustawy o KSC | W związku z poszerzeniem katalogu podmiotów krajowego systemu cyberbezpieczeństwa weryfikacji wymaga zakres właściwości poszczególnych CSIRT poziomu krajowego, o którym mowa w art. 26 ust. 5-7 ustawy o KSC. Przykładowo, zgodnie z art. 26 ust. 6 ustawy o KSC, do zadań CSIRT NASK należy koordynacja obsługi incydentów zgłaszanych przez jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2-6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Tymczasem zgodnie z art. 4 ustawy o KSC, podmioty, o których mowa w art. 9 pkt 11 i 12 ustawy o finansach publicznych – czyli uczelnie publiczne oraz Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne – nie zostały objęte odesłaniem do art. 9 pkt 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych. Na gruncie ustawy o KSC funkcjonują jako podmioty systemu szkolnictwa wyższego na mocy odesłania do art. 7 ust. 1 pkt 1 i 3-7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce. Katalog z art. 7 ustawy – Prawo o szkolnictwie wyższym i nauce obejmuje również instytuty badawcze, takie jak instytuty naukowe PAN, instytuty badawcze, działające na podstawie ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, międzynarodowe instytuty naukowe utworzone na podstawie odrębnych ustaw działające na terytorium Rzeczypospolitej Polskiej, Centrum Łukasiewicz, działające na podstawie ustawy z dnia 21 lutego 2019 r. o Sieci Badawczej Łukasiewicz, instytuty działające w ramach Sieci Badawczej Łukasiewicz oraz Polską Akademię Umiejętności. Tymczasem art. 26 w ust. 6 pkt 1 lit. c ustawy o KSC wskazuje jedynie, że zakresem właściwości CSIRT NASK są objęte instytuty badawcze – bez odwoływania się do specyfiki tych instytutów określonej w art. 7 ustawy – Prawo o szkolnictwie wyższym i nauce, co może powodować trudności interpretacyjne. Kwestia ta wymaga uzupełnienia. Podobnie nie zostało rozstrzygnięte do właściwości którego z CSIRT poziomu krajowego należeć będzie obsługa incydentów zgłaszanych przez osobno wskazane w art. 4: Wody Polskie oraz Polski Funduszu Rozwoju (art. 1 pkt 4 lit. d projektu ustawy zmieniającej). Ogólny przepis art. 26 ust. 6 pkt 1 lit. k ustawy o KSC wskazujący na właściwość CSIRT NASK w zakresie innych podmiotów niż wymienione w lit. a-j i ust. 5 i 7 art. 26 nie jest w tym przypadku wystarczający. Weryfikacji wymaga również zakres właściwości przekazanej w drodze porozumienia pomiędzy poszczególnymi CSIRT na podstawie art. 26 ust. 10 i 11 ustawy o KSC. Sugeruje się przegląd zawartych porozumień celem dostosowania właściwości rzeczowej CSIRT poziomu krajowego, która jest określona w ustawie do zakresu faktycznie wykonywanych zadań. Nie kwestionując możliwości zawarcia porozumień, co do zakresu zadań wykonywanych na rzecz niektórych podmiotów, zwłaszcza w przypadku powstania nowych kategorii podmiotów objętych krajowym systemem cyberbezpieczeństwa, zasadnym wydaje się dostosowanie przepisów ustawy do praktyki jej stosowania wynikającej z zawartych porozumień. Kwestię te pozostawia się jednakże do decyzji merytorycznej projektodawcy. W razie wzięcia pod uwagę tego problemu, konieczne będzie uzupełnienie projektu o stosowne przepisy przejściowe i dostosowujące dotyczące zwartych porozumień ich utrzymania, uchylenia czy wygaszenia. | Rozstrzygnięcie właściwości CSIRT poziomu krajowego dla:  1. podmiotów systemu szkolnictwa wyższego i nauki  2. Państwowego Gospodarstwa Wodnego „Wody Polskie”  3. Polskiego Funduszu Rozwoju  4. Rozstrzygnięcie o właściwości CSIRT w kontekście porozumień zawartych pomiędzy CSIRT poziomu krajowego. | **Uwaga uwzględniona**  Przepis zostanie poprawiony.  Modelowo – szkolnictwo, Wody Polskie czy Polskie Fundusz Rozwoju powinny zgłaszać do CSIRT NASK, chyba, że będą operatorami infrastruktury krytycznej. |
|  | **RCL** | Relacja do ustawy o ponownym wykorzystywaniu informacji sektora publicznego, art. 37 ustawy o KSC | W związku z szeroką definicją pojęcia „informacja sektora publicznego”, które jest projektowane w ustawie o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego,[ *informacja sektora publicznego – każdą treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będącą w posiadaniu podmiotu zobowiązanego]* oraz faktem, że katalog podmiotów zobowiązanych do udostępniania informacji sektora publicznego pokrywa się z katalogiem podmiotów objętych systemem cyberbezpieczeństwa wymaga analizy możliwość wyłączenia stosowania przepisów ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego do części informacji będących w posiadaniu podmiotów zobowiązanych dotyczących cyberbezpieczeństwa. Definicja informacji sektora publicznego nie wiąże tego pojęcia z zakresem pojęcia „informacja publiczna” w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Tym samym nie będzie wystarczające wyłączenie stosowanie ustawy o dostępie do informacji publicznej, o którym mowa w art. 37 ustawy o KSC. Ustawa o KSC nie formułuje także osobnej definicji prawnie chronionej tajemnicy w zakresie cyberbezpieczeństwa, a zatem informacje te nie będą objęte wyłączeniem dotyczącym tych tajemnic zawartym w projekcie ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego. | Wyłączenie informacji przetwarzanych przez poszczególne podmioty systemu cyberbezpieczeństwa lub poszczególnych kategorii informacji sektora publicznego z możliwości ich ponownego wykorzystywania. Wyłączenie to jak się wydaje nie powinno obejmować danych stanowiących informacji publiczną, które są publikowane w BIP. | **Uwaga uwzględniona**  Zostanie dodany przepis. |
|  | **RCL** | Art. 39 ustawy o KSC | W związku z wprowadzeniem CSIRT sektorowych oraz ISAC i SOC wymaga analizy czy przepis art. 39 dotyczący przetwarzania danych o incydentach, w tym danych osobowych, nie wymaga uzupełnienia o zadania realizowane przez CSIRT sektorowe, ISAC czy SOC. Zwłaszcza w kontekście przetwarzania danych osobowych. | Przeanalizowanie przepisów pod kątem nowych zadań i nowych podmiotów oraz ewentualne uzupełnienie odesłań w art. 39 ustawy o KSC lub stworzenie osobnej regulacji dotyczącej przetwarzania danych, w tym danych osobowych przez SOC i ISAC. | **Wyjaśnienie**  Przepisy zostały ponownie przeanalizowane.  Należy wyjaśnić, że ISAC nie będą przetwarzać informacji o incydentach. Natomiast SOC przetwarzają incydenty dotyczące operatora usługi kluczowej, na którego rzecz działają, zgodnie z umową.  Z kolei CSIRT sektorowe będą przetwarzać informacje o incydentach – odpowiednio jest zmieniany art.. 39. |
|  | **RCL** | Rozdział 11a. Krajowy system certyfikacji cyberbezpieczeństwa | W opisanej procedurze dotyczącej zatwierdzenia certyfikatu (art. 59o i art. 59q ustawy o KSC) projektodawca posługuje się pojęciem „przesłania” i „doręczenia” nie precyzując jednak w jakim trybie następuje przesłanie wniosku oraz doręczenia decyzji. Czy odnosi się ono do doręczenia za pośrednictwem operatora pocztowego czy przy użyciu środków komunikacji elektronicznej.  Podobnie rozstrzygnięcia wymagają kwestie proceduralne dotyczące sposobu informowania o cofnięciu certyfikatu przez jednostkę oceniającą zgodność (art. 59u ustawy o KSC).  Upoważnienie ustawowe z art. 59w ustawy o KSC, przekazujące do uregulowania w drodze rozporządzenia wysokość opłat za zatwierdzenie certyfikatu, może wymagać uzupełnienia, gdyż przepisy ustawy nie rozstrzygają sposobu czy trybu wnoszenia takiej opłaty.  W zakresie art. 59za ustawy o KSC, który wskazuje, że jednostki oceniające zgodność publikują na swojej stronie internetowej „procedurę postępowania ze skargami, o których mowa w art. 63 rozporządzenia 2019/881” (art. 59za ust. 1 ustawy o KSC) i „informują o prawie do skierowania sprawy do sądu” (art. 59za ust. 4) ustawa powinna przesądzać do jakiego sądu może być skierowana taka sprawa (powszechnego czy administracyjnego), a co a tym idzie w jakiej procedurze będzie rozpatrywana. Procedurę administracyjną (zgodnie z ar. 59zc ustawy o KSC) stosuje się jedynie do skarg na jednostkę oceniającą zgodność kierowanych do ministra właściwego do spraw informatyzacji. | Uzupełnienie regulacji o przepisy proceduralne dotyczące sposobu wnoszenia wniosku i sposobu dokonywania doręczeń lub o stosowne odesłanie.  Analiza i ewentualne uzupełnienie upoważnienia ustawowego.  Określenie sądu właściwego, procedury i trybu rozpoznawania spraw związanych, ze skargami o których mowa w art. 63 rozporządzenia 2019/881. | **Uwaga uwzględniona**  Przepisy dotyczące przesłania wniosku oraz doręczenia decyzji zostaną doprecyzowane.  Delegacja ustawowa zostanie doprecyzowana.  Skargi, o których mowa w art. 63 rozporządzenia 2019/881 będą rozpatrywane przez sądy cywilne.  Wyjaśnić należy, że w zakresie art. 59za należy wskazać, że jednostki oceniające zgodność będą prowadziły swoje działania na podstawie umów zawartych ze swoimi klientami. Dlatego też potencjalne skargi będą dotyczyć kwestii stanowiących równocześnie niewłaściwe wykonanie umowy i na tej podstawie będzie podlegać ogólnym przepisom o drodze sądowej. Sprawy te będą w tym zakresie rozstrzygane przez sądy cywilne. Wstąpienie na drogę sądową nie będzie również uzależnione od wcześniejszego wykorzystania procedury skargowej. Każdorazowo klient będzie mógł zdecydować czy chce skorzystać z wewnętrznej procedury danego podmiotu czy też skierować sprawę na drogę sądową. |
|  | **RCL** | Rozdział 11b. Operator sieci komunikacji strategicznej | Szczegółowego uzasadnienia wymaga umieszczenie regulacji dotyczących operatora sieci komunikacji strategicznej w ustawie o krajowym systemie cyberbezpieczeństwa, nie natomiast w ustawie – Prawo telekomunikacyjnej lub ustawie o zarządzaniu kryzysowym. Art. 59zd ustawy o KSC wskazuje, że zadania operatora sieci komunikacji strategicznej odnoszą się do „(…) zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji”. Nie dotyczą zatem zadań z zakresu krajowego systemu cyberbezpieczeństwa. Nie kwestionując związku funkcjonalnego pomiędzy zapewnieniem bezpieczeństwa sieci telekomunikacyjnej a wykonywaniem zadań dotyczących cyberbezpieczeństwa przepisy ustawy powinny wskazywać jakie zadania z zakresu krajowego systemu cyberbezpieczeństwa wykonuje operator sieci strategicznej. Należy również zauważyć, że zgodnie z art. 2 ust. 2 pkt 1 ustawy o KSC nie stosuje się do przedsiębiorców telekomunikacyjnych w zakresie wymogów bezpieczeństwa i zgłaszania incydentów, zaś operator sieci strategicznej zgodnie z projektowanymi przepisami jest przedsiębiorcą telekomunikacyjnym. Odesłania do przepisów Prawa telekomunikacyjnego (np.: w projektowanym art. 59ze) oraz wskazanie, że w razie niezawarcia umowy o dostęp do sieci telekomunikacyjnej przez operatora telekomunikacyjnego Prezes UKE wydaje decyzję w tym zakresie, wskazują, że przepisy te należy wiązać z wykonywaniem zadań na rzecz obronności i bezpieczeństwa państwa przez operatorów telekomunikacyjnych. Przepisy te regulował dotychczas dział VIII ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne pt. „Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego”. W projektowanych przepisach pojawiają się także pojęcia i zadania dotyczące „ zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej”, a zatem powiązane z wykonywaniem zadań na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Wymaga zatem wyjaśnienia czy projektowane przepisy nie stanowią materii ustawy – Prawo telekomunikacyjnej lub ustawy o zarządzaniu kryzysowym. | Przedstawienie szczegółowego wyjaśnienia oraz powiązanie regulacji zgodnie z jej zakresem przedmiotowym, na poziomie normatywnym, z wykonywaniem zadań z zakresu cyberbezpieczeństwa. | **Wyjaśnienie**  Przepisy dotyczące operatora sieci komunikacji strategicznej mają zapewnić bezpieczną łączność rządową za pomocą nowoczesnych technologii w tym także za pomocą systemów teleinformatycznych.  Operator sieci komunikacji strategicznej będzie zapewniał wyższy poziom cyberbezpieczeństwa (w szczególności wyższej dostępności) usług świadczonych dla administracji rządowej. Nie będzie on świadczył usług komercyjnych. Dlatego zasadne jest umieszczenie tych przepisów w ustawie o krajowym systemie cyberbezpieczeństwa. |
|  | **RCL** | Art. 62a ustawy o KSC | Przepisy dotyczące przyznawania dodatkowego wynagrodzenia dla osób zatrudnionych przy wykonywaniu zadań dotyczących cyberbezpieczeństwa wymagają korekty. Z przepisów nie wynika, czy dodatkowe wynagrodzenie ma charakter jednorazowy, stanowi dodatek do wynagrodzenia zasadniczego, stanowi dodatek za wykonywanie konkretnego zadania czy ma charakter stały, wypłacany miesięcznie? Budzi wątpliwości umieszczenie tej regulacji w przepisach ustawy o krajowym systemie cyberbezpieczeństwa, bez odniesienia zasad i trybu przyznawania tego wynagrodzenia w przepisach stanowiących podstawę wynagradzania dla osób zatrudnionych w tych podmiotach. Może to rodzić trudności w ich stosowaniu, gdyż na podstawie projektowanego aktu nie można przesądzić czy podstawą do wypłaty dodatkowych środków będzie zawierana dodatkowo umowa (nie przesądzając o dopuszczalności jej zawarcia w poszczególnych podmiotach), fakt wykonywania zadań, wydane polecenie w tym zakresie czy sam fakt zajmowania stanowiska związanego z cyberbezpieczeństwem? Podobnie nie został przesądzony charakter tego świadczenia z punktu widzenia przepisów dotyczących ubezpieczenia społecznego oraz pobierania zaliczki na podatek dochodowy czy wliczania ich wysokości do obliczania innych świadczeń pracowniczych, zależnych od średniego wynagrodzenia w danym okresie (np.: dodatkowe wynagrodzenie roczne). Kwestie te mogą wymagać odrębnego uregulowania w przypadku każdego pracodawcy, należy zatem powiązać te regulacje z przepisami dotyczącymi zasad zatrudniania i wynagradzania w tych jednostkach.  Ponadto budzi wątpliwości wskazanie w normie ustawowej liczby osób, którym takie dodatkowe wynagrodzenie przysługuje. Nie wskazano jak ten limit przełoży się na możliwość przyznawania wynagrodzenia i finansowania w poszczególnych podmiotach: CSIRT NASK, CSIRT MON, ABW oraz w urzędzie obsługującym Pełnomocnika. Normy ustawowe powinny w sposób abstrakcyjny i generalny ustalać warunki przyznawania takiego wynagrodzenia, kwestie zaś limitowania środków i ich podziału na etaty powinny zostać powiązane z zasadami finansowania poszczególnych jednostek oraz obsadzania stanowisk w tych jednostkach. | Powiązanie wynagrodzenia dodatkowego z przepisami normującymi pierwotnie zasady zatrudnienia oraz przyjęcia do służby, a także wynagradzania osób zatrudnionych w CSIRT NASK, CSIRT MON i CSIRT GOV oraz urzędzie obsługującym Pełnomocnika do wskazanych zadań. | **Uwaga częściowo uwzględniona**  Przepis zostanie poprawiony.  Zostanie wskazane, że będzie to stałe, dodatkowe wynagrodzenie miesięczne. |
|  | **RCL** | art. 62b ustawy o KSC | Uregulowanie wskazujące, że w Dzienniku Urzędowym RP „Monitor Polski” zamieszczane są ogłoszenia zawierające odnośnik do strony internetowej zawierającej treść rekomendacji dotyczących „podejmowania środków technicznych i organizacyjnych mających na celu zwiększenie cyberbezpieczeństwa” budzi wątpliwości. Celem publikowania w dzienniku urzędowym jest praktyczna realizacji konstytucyjnej zasady pewności prawa i zaufania obywateli do państwa przez utrwalenie w sposób nie budzących wątpliwości treści aktów władzy publicznej. Mając na uwadze, że rekomendacje będą skierowane do podmiotów krajowego systemu cyberbezpieczeństwa, a zatem również podmiotów które nie są podmiotami publicznymi (takich jak ISAC czy SOC), zamieszczenie ogłoszenia z odnośnikiem do strony internetowej, która będzie zawierała treść rekomendacji wydaje się nie realizować ww. celu publikacji. Należy podnieść, że treść publikacji na stronie internetowej będzie mogła podlegać modyfikacjom niezależnie od opublikowania odnośnika do jej adresu w Dzienniku Urzędowym RP „Monitor Polski”. Na gruncie projektowanych przepisów nie będzie możliwe ustalenie, w sposób niebudzący wątpliwości, treści rekomendacji na podstawie ogłoszenia opublikowanego w Dzienniku Urzędowym. Dodatkowych, szczegółowych ustaleń wymagają również kwestie techniczne związane z tą publikacją Niezależnie od powyższego należy zauważyć, że projektowane przepisy nie wskazują czy treść rekomendacji może podlegać zmianom oraz czy czas stosowania tych rekomendacji jest określony, a także czy informacja o takiej zmianie jest publikowana, podobnie jak informacja o wygaśnięciu danej rekomendacji. | Ponowna analiza i zmiana przepisów. | **Uwaga uwzględniona**  Rekomendacje będą publikowane nie w Monitorze Polskim tylko w Biuletynie Informacji Publicznej. |
|  | **RCL** | Art. 66b ust. 3 ustawy o KSC | Zgodnie z projektowaną regulacją „3. Podmioty o których mowa w art. 66 ust. 1 pkt 1-4, do których stosuje się ustawa – Prawo zamówień publicznych, nie dokonują zamówień sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 8”, a zatem decyzji o uznaniu dostawcy usług lub oprogramowania za dostawcę wysokiego ryzyka. Przepis budzi wątpliwości, gdyż sformułowanie „nie dokonuje zamówień” nie precyzuje jaki skutek dla postępowania w sprawach zamówień publicznych wywołuje decyzja o uznaniu dostawcy za podmiot wysokiego ryzyka. Skutek ten będzie się różnił w zależności od etapu postępowania o udzielenie zamówienia publicznego. W tym kształcie regulacja nie przesądza czy zamawiający powinien umorzyć postępowanie w sprawie zamówienia publicznego (wówczas należałoby uzupełnić przesłanki umorzenia postępowania zawarte w ustawie PZP), odrzucić ofertę wykonawcy, który został uznany za dostawcę wysokiego ryzyka (wówczas koniecznym wydaje się uzupełnienie przesłanek odrzucenia oferty), ani nie wskazuje jaki skutek wywołuje uznanie dostawcy za dostawcę wysokiego ryzyka w sytuacji, w której została zawarta umowa, która przewiduje realizację zamówienia w częściach albo umowa periodyczna. Czy umowa ta powinna zostać wypowiedziana, i wszczęte nowe postępowanie w sprawie o udzielenie zamówienia publicznego czy też umowa ta może być kontynuowana aż do upływu okresu, w którym dany sprzęt lub oprogramowanie powinny zostać wycofane?  Należy również podnieść, że zaproponowana redakcja przepisu wydaje się nieadekwatna do jej celu. Przyjmując, że celem regulacji jest ograniczenie możliwości nabywania sprzętu lub oprogramowania, które zostały objęte decyzją, o której mowa w art. 66a ust. 8 ustawy o KSC, to nie ma znaczenia w jakiej procedurze nabywana jest ten sprzęt lub oprogramowanie i czy podmiot stosuje do tej procedury zakupu postępowanie w sprawach zamówień publicznych. Przepis w takim przypadku powinien stanowić o niemożliwości zakupu przedmiotów objętych decyzją z art. 66a ust. 8 ustawy o KSC. | Przepis wymaga ponownej analizy, w szczególności co do trafności przyjętego rozwiązania, i korekty. | **Uwaga uwzględniona**  Przepis zostanie zmieniony.  Przepis będzie stanowił o niemożliwości zakupu przedmiotów objętych decyzją z art. 66a ust. 8 ustawy o KSC. |
|  | **RCL** | Art. 66d ustawy o KSC | Przepisy dotyczące ograniczenia zakresu doręczanego uzasadnienia wyroku oraz wyłączenia możliwości wstrzymania natychmiastowej wykonalności decyzji o uznaniu dostawcy usług za podmiot wysokiego ryzyka wymagają ponownej analizy w zakresie spójności z regulacjami ustawy – Prawo o postępowaniu przed sądami administracyjnymi i ustawą o ochronie informacji niejawnych. Niezależnie od dopuszczalności ograniczenia doręczenia pocztowego ze względu na ochronę informacji niejawnych, z uwagi na prawo do rzetelnego postępowania, strona nie powinna być ograniczona w samym dostępie do uzasadnienia rozstrzygnięcia podejmowanego przez sąd, aby mieć możliwość ich zaskarżenia. | Przepisy wymagają ponownej analizy, w szczególności co do trafności przyjętego rozwiązania, i ewentualnej korekty. | **Wyjaśnienie**  KPRM przeanalizuje jeszcze raz te przepisy. Preferowany jest model udostępniania uzasadnienia i decyzji. |