Nazwa projektu Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i niektórych innych ustaw **Ministerstwo wiodące i ministerstwa współpracujące** Kancelaria Prezesa Rady Ministrów **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński, Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów **Kontakt do opiekuna merytorycznego projektu** Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 12 października 2021 r. **Źródło:** Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15) **Nr w wykazie prac legislacyjnych i programowych Rady Ministrów** UD68

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawa o krajowym systemie cyberbezpieczeństwa (zwana dalej „ustawą o KSC"), przyjęta w 2018 r., stanowi implementację dyrektywy NIS i tworzy podstawy prawno-organizacyjne systemu cyberbezpieczeństwa na poziomie krajowym. Krajowy system cyberbezpieczeństwa składa się z wielu podmiotów. Przede wszystkim są to operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa systemów informacyjnych, utrzymania niezakłóconego świadczenia usług, a także zgłaszania i obsługi incydentów bezpieczeństwa. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów, które zostały wskazane w załączniku nr 1 do ustawy. Ustawa określa 6 kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa sektorów gospodarki tj.: energii, transportu, zdrowia, bankowości i infrastruktury rynków finansowych, zaopatrzenia w wodę oraz infrastruktury cyfrowej. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa (zwany dalej „organem właściwym"), który odpowiada za wyznaczanie operatorów oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze. Obecnie w krajowym systemie cyberbezpieczeństwa nie znajdują się przedsiębiorcy telekomunikacyjni, ani dostawcy usług zaufania.

Zespoły CSIRT

Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej „CSIRT") poziomu krajowego. Do zadań zespołów CSIRT poziomu krajowego należy także klasyfikowanie incydentów jako krytyczne. Ustawa usankcjonowała istnienie trzech zespołów – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej - Państwowym Instytucie Badawczym, zwanym dalej „NASK") oraz CSIRT MON (działającego w Ministerstwie Obrony Narodowej). Ustawa klarownie określa zakres kompetencyjny oraz podmiotowy wskazany dla danego zespołu CSIRT poziomu krajowego. CSIRT GOV koordynuje obsługę incydentów zgłoszonych m.in. od podmiotów administracji rządowej oraz operatorów infrastruktury krytycznej. CSIRT MON, jest właściwy do podmiotów podległych resortowi obrony narodowej. Natomiast CSIRT NASK posiada najszerszy zakres podmiotowy od operatorów usług kluczowych m.in. w sektorze bankowości po jednostki samorządu terytorialnego. Zespoły

CSIRT współpracują ze sobą na bieżąco w oparciu o procedury operacyjne. Ponadto, w przypadku wystąpienia incydentu krytycznego, zespoły CSIRT współpracują ze sobą w ramach Zespołu do spraw Incydentów Krytycznych.

Sektorowe zespoły cyberbezpieczeństwa
Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za obsługę lub wsparcie obsługi incydentów w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko jeden taki zespół - CSIRT KNF dla sektora bankowości i infrastruktury rynków finansowych, w Urzędzie Komisji Nadzoru Finansowego.

Pełnomocnik
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, zwany dalej „Pełnomocnikiem", jest odpowiedzialny za koordynowanie na poziomie krajowym realizacji zadań dotyczących cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu lub podsekretarza stanu, jest powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy również analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników, opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT, jak również nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

Kolegium
Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium", jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje również kwestie cyberbezpieczeństwa dotyczące decyzji Prezesa UKE w sprawie rezerwacji częstotliwości. Na czele Kolegium stoi Prezes Rady Ministrów, a w jego skład – jako stali członkowie - wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych (ww. ministrowie mogą być reprezentowani przez swoich zastępców), Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz Sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów może wydać wiążące wytyczne w celu koordynacji działań w zakresie cyberbezpieczeństwa.

Doświadczenia z funkcjonowania krajowego systemu cyberbezpieczeństwa
Dwa lata doświadczeń na poziomie krajowym (od 2018 r. – wejście w życie ustawy o KSC) pozwoliły ocenić skuteczność wdrożonych rozwiązań prawno-organizacyjnych oraz zidentyfikować obszary wymagające zmian ustawowych, które usprawniają funkcjonowanie systemu cyberbezpieczeństwa m.in. konieczność ujednolicenia na poziomie krajowym procedur zgłaszania incydentów, przyspieszenie tworzenia sektorowych zespołów cyberbezpieczeństwa, czy umożliwienia tworzenia centrów analizy i wymiany informacji (ISAC).

Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były dotychczas powoływane. Dotychczas powstał tylko jeden sektorowy CSIRT w sektorze finansowym – CSIRT-KNF. Wzrasta liczba incydentów cyberbezpieczeństwa i cyberzagrożeń, co sprawia, że zachodzi konieczność ustanowienia takich zespołów dla każdego z sektorów lub podsektorów kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa i obywateli. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z cyberzagrożeniami oraz otrzymają bezpośrednie wsparcie w skutecznej reakcji na incydenty.
Ponadto, wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo (a także podmioty świadczące usługi z zakresu cyberbezpieczeństwa) nie współpracują ze sobą, co skutkuje brakiem przepływu istotnych informacji między podmiotami systemu. Operatorzy usług kluczowych mają trudności ze spełnieniem wyśrubowanych wymogów technicznych dla wewnętrznych struktur cyberbezpieczeństwa.
Należy również wskazać na konieczność uregulowania zasad współpracy pomiędzy podmiotami publicznymi funkcjonującymi na poziomie województwa. W informacji o wynikach kontroli Najwyższej Izby Kontroli z 2019 r.

negatywnie ocenione aż 70% kontrolowanych jednostek samorządu terytorialnego (JST) w zakresie wykonywania zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji. NIK zalecił Ministrowi Cyfryzacji szeroką promocję wśród organów administracji wiedzy o wymogach w zakresie bezpieczeństwa informacji. Co więcej, szereg incydentów bezpieczeństwa, które miały miejsce w JST w ostatnim czasie m.in. w Kościerzynie oraz Lututowie, pokazują, że zapewnienie odpowiedniej reakcji (w tym koordynacji działań) na poziomie województwa jest krytyczne.
Do tej pory powstało w Polsce tylko 1 centrum wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa – ISAC-Kolej, które rozpoczęło działalność w październiku 2020 r. ISAC (Information Sharing and Analysis Center, centrum wymiany informacji i analiz) gromadzi informacje o podatnościach i cyberzagrożeniach. Taka formuła znacząco wpływa na poprawę cyberbezpieczeństwa. Wskazane jest, aby więcej takich organizacji powstało w Polsce.

W celu wykonywania specjalistycznych analiz z zakresu cyberbezpieczeństwa oraz przygotowywania rekomendacji, zaleceń bezpieczeństwa, niezbędne jest posiadanie wysoko wykwalifikowanej kadry eksperckiej o unikalnych kompetencjach m.in. z zakresu Cyber Threat Intelligence, czy analizy złośliwego oprogramowania. Obecne środki budżetowe nie pozwalają na zatrudnienie takich osób po stawkach rynkowych w instytucjach publicznych, co powoduje, że zespoły CSIRT poziomu krajowego mają ograniczoną możliwość pozyskiwania specjalistycznej kadry.

Zauważono również, że uprawnienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa są niewystarczające dla zadań, które musi wypełniać. Brakuje mu skutecznych środków oddziaływania na podmioty krajowego systemu cyberbezpieczeństwa, w tym przede wszystkim wydawania ostrzeżeń w sytuacji prawdopodobieństwa wystąpienia incydentu krytycznego. Chodzi o podobny instrument jaki jest m.in. w Czechach, czyli ostrzeżenie szefa agencji NUKIB.

Brakuje również środka prawnego, który umożliwiałby wydawanie rekomendacji o charakterze technicznym (w tym zakresie Narodowych Standardów Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa RP na lata 2019-2024) i jednocześnie obowiązku uwzględnienia tych rekomendacji przez podmioty krajowego systemu cyberbezpieczeństwa w trakcie procesu zarządzania ryzykiem.

Zmiany na poziomie UE
Ponadto, w tym samym okresie doszło do istotnych zmian w prawie europejskim. Jednym z priorytetów Komisji Europejskiej stało się zapewnienie cyberbezpieczeństwa sieciom telekomunikacyjnym. Weszła w życie nowa regulacja – dyrektywa Europejski Kodeks Łączności Elektronicznej (EKŁE), który umożliwia (w odróżnieniu od poprzedniej regulacji tzw. dyrektywy ramowej) uspójnienie procedury zgłaszania i reagowania na incydenty na poziomie krajowym. O tej możliwości, czyli zharmonizowaniu procedury zgłaszania incydentów w rozumieniu ustawy o KSC, z incydentami raportowanymi przez przedsiębiorców telekomunikacyjnych wskazuje się także w niedawno opublikowanym eksperckim opracowaniu „Synergies in Cybersecurity Incident Reporting". Jest to dokument przygotowany przez Grupę Współpracy NIS we współpracy z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa, zwanej dalej „ENISA" oraz Komisję Europejską. Opracowanie wprost wskazuje, że państwa mogą dokonać harmonizacji procedur z dyrektywy NIS, EKŁE oraz rozporządzenia eIDAS, dzięki m.in. posiadaniu podobnej taksonomii w klasyfikacji incydentów, konieczności określenia progów incydentów. Co więcej podkreślono fakt, że usługi objęte tymi trzema reżimami prawnymi mają krytyczne znaczenie dla naszych społeczeństwa.
EKŁE nie jest jedynym symbolem zmian w postrzeganiu przez Komisję Europejską bezpieczeństwa w sektorze telekomunikacyjnym. Komisja wielokrotnie m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G, podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie tego znajduje swój wymiar w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, określanego jako 5G Toolbox[1]. Zestaw obejmuje zarówno narzędzia o charakterze strategicznym i technicznym, jak również te o charakterze wspierającym. Cele są dwa: po pierwsze, bezpieczeństwo sieci 5G, a po drugie: uspójnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox zawiera też m.in. definicje zestawu środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą kręgosłupem Jednolitego Rynku Cyfrowego UE. Są środki o charakterze:

[1] *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures,* https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

- Strategicznym - m.in. większe uprawnienia dla organów właściwych, w tym ocena bezpieczeństwa łańcucha dostaw, większe wymagania dla przedsiębiorców telekomunikacyjnych oraz ocena ryzyka dostawców sprzętu lub oprogramowania,
- Technicznym –m.in. badanie bezpieczeństwa oprogramowania i urządzeń – uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego: CSIRT GOV, CSIRT MON, CSIRT NASK – wynikające z art. 33 ustawy o KSC,
- Wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa

Pakiet cyberbezpieczeństwa UE

16 grudnia 2020 r. Komisja Europejska opublikowała cały pakiet dokumentów, które ukształtują europejski ekosystem cyberbezpieczeństwa w kolejnej dekadzie. Jednym z elementów wchodzących w skład tego pakietu jest nowa Strategia Cyberbezpieczeństwa Unii Europejskiej - The EU's Cybersecurity Strategy for the Digital Decade[2].

Proponowane obszary interwencji i działań wzmacniających europejski system cyberbezpieczeństwa dotyczą m.in.:

- Stworzenia sieci operacyjnych centrów bezpieczeństwa (SOC) w UE. Sieci, która będzie wspierana przez innowacyjne technologie oparte m.in. o sztuczną inteligencję,
- Położony zostanie nacisk na wsparcie małych i średnich przedsiębiorstw, w tym działania dot. podniesienia świadomości, wiedzy i kompetencji pracowników.
- Rozbudowa zdolności operacyjnych na poziomie UE poprzez utworzenie Joint Cyber Unit (Wspólnego zespołu operacyjnego) odpowiedzialnego m.in. za przeciwdziałanie, odstraszaniu i reagowaniu na cyberataki.
- Wzmocniony zostanie mechanizm unijnych sankcji wobec podmiotów, w tym państwowych, przeprowadzających cyberataki.
- Zwrócono szczególna uwagę na sprawne wdrożenie zaleceń z 5G Toolbox we wszystkich państwach członkowskich.

Krajowy System Certyfikacji Cyberbezpieczeństwa

Projektowana ustawa pozwala dostosować polski porządek prawny do obowiązków wynikających z wejścia w życie (w czerwcu 2019 r.) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, zwanego dalej Aktem o Cyberbezpieczeństwie. Stanowi również realizację celu 2. Strategii Cyberbezpieczeństwa rzeczypospolitej Polskiej na lata 2019-2024 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Szczególnie istotną kwestią jest tu dostosowanie definicji zawartych w ustawie o KSC do zmian, jakie zaszły w tej dziedzinie na poziomie europejskim. Prawo europejskie wprowadziło cały szereg nowych pojęć oraz dokonało aktualizacji już istniejących. Dostosowanie do tych zmian jest więc konieczne zarówno ze względu na konieczność zachowania spójności porządku prawnego jak również ze względu na korzyści wynikające z posiadania jednolitej terminologii z partnerami z Unii Europejskiej.

Rola sieci i systemów teleinformatycznych wzrosła niepomiernie w ostatnich latach sprawiając, że stały się one niezbędnym elementem współczesnej gospodarki. W związku z pandemią koronawirusa proces ten zapewne będzie postępował coraz szybciej. Jako, że społeczeństwa coraz bardziej będą polegały na produktach i usługach funkcjonujących w cyberprzestrzeni, tym istotniejsze staje się zapewnienie bezpieczeństwa działań podejmowanych w tej płaszczyźnie. Wprowadzenie jednolitych zasad przyznawania certyfikatów cyberbezpieczeństwa i ich wzajemne uznanie w państwach Unii Europejskiej zapewnią, że przedsiębiorstwa będą w stanie lepiej zabezpieczyć swoje interesy w cyberprzestrzeni. Ponadto wzajemne uznawanie certyfikatów zapewni im lepszą pozycję do konkurencji na rynku europejskim. Działania te przyczynią się do ogólnego wzrostu bezpieczeństwa w cyberprzestrzeni. Posłużą też uporządkowaniu rynku w tym zakresie oraz objęciu

[2] *The EU's Cybersecurity Strategy for the Digital Decade*, https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.

procesów certyfikacji nadzorem. Wyraźne wsparcie państwa w zakresie certyfikacji powinno również przyczynić się do zwiększenia świadomości społecznej w kwestii cyberbezpieczeństwa.

Szybkie przyjęcie proponowanych przepisów może dać polskim przedsiębiorcom dużą szansę do pozyskania klientów z sąsiednich krajów zainteresowanych certyfikacją ich produktów. Będzie to więc szansą dla znacznego poszerzenia bazy potencjalnych klientów.

Sama certyfikacja w zakresie cyberbezpieczeństwa jest procesem czasochłonnym i kosztownym, co ogranicza dostępność do certyfikatów. Wprowadzenie krajowego systemu certyfikacji powinno przyczynić się do zmiany tego stanu rzeczy.

Przyjęte w ustawie rozwiązania umożliwiają również tworzenie krajowych programów certyfikacyjnych. Dzięki temu możliwe będzie zwiększenie cyberbezpieczeństwa w obszarach uznanych za kluczowe.
Dzięki przepisom umożliwiającym tworzenie krajowych programów certyfikacji cyberbezpieczeństwa administracja publiczna uzyska skuteczne narzędzie pozwalające reagować na cyberzagrożenia dotyczące konkretnych produktów, usług czy procesów. Możliwe będzie opracowanie programu certyfikacji, które weźmie te zagrożenia pod uwagę bez konieczności oczekiwania na działania na forum Unii Europejskiej.

Rewolucja informatyczna i rozwój sieci komputerowych spowodowały istotne uzależnienie działania Państwa od sprawnych, bezpiecznych systemów teleinformatycznych i sieci telekomunikacyjnych. Bezpieczne systemy łączności strategicznej, spajającej działania administracji publicznej i zapewniające sprawne działanie ePaństwa są niezwykle ważnym elementem dobrze funkcjonującego państwa.
Należy brać przykład z najlepszych praktyk krajów europejskich. W Austrii, Belgii, Finlandii, Francji, Niemczech, czy na Węgrzech, zarządzanie sieciami w warstwie bezpieczeństwa oraz w warstwie aplikacyjnej realizowane jest przez wyspecjalizowane jednostki państwowe lub operatorów państwowych. Jednocześnie w państwach członkowskich Unii Europejskiej funkcjonują różne modele własności infrastruktury sieciowej. Warstwa szkieletowa i dystrybucyjna sieci krytycznych może być bezpośrednio lub pośrednio własnością państwa (Finlandia, Węgry, częściowo Francja i Belgia) lub może być dzierżawiona w formie usług transmisji danych lub ciemnych włókien od kwalifikowanych operatorów komercyjnych. Dostawcy ci są na ogół wybierani w postępowaniach zamkniętych, na podstawie specjalnych aktów prawnych (dekretów, ustaw) bądź w trybie negocjacji. Podobnie nabywane są usługi integracyjne i usługi wsparcia technicznego (utrzymanie sieci). Przepisy stanowiące podstawę prawną dla pomięcia trybów konkurencyjnych powołują się artykuł 346 Traktatu o funkcjonowaniu Unii Europejskiej, który zezwala krajom członkowskim na samodzielne kształtowanie polityki zakupowej w sprawach dotyczących obronności kraju.
Projekt ustawy o strategicznej sieci bezpieczeństwa zakłada utworzenie takiej sieci, będącej bezpieczną i niezawodną siecią telekomunikacyjną wykorzystywaną do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Sieć ta będzie zarządzana przez Operatora strategicznej sieci bezpieczeństwa, dalej „OSSB", wskazywanego, w drodze zarządzenia, przez Prezesa Rady Ministrów spośród podmiotów spełniających wymogi ustawowe.

Projektowana ustawa w zakresie, w jakim przewiduje utworzenie operatora strategicznej sieci bezpieczeństwa zapewni funkcjonowanie operatora telekomunikacyjnego, który świadczyć będzie usługi telekomunikacyjne dla najważniejszych osób w państwie oraz jednostkom i służbom podległym oraz nadzorowanym przez Ministra Obrony Narodowej, administracji rządowej, a także dla instytucji i przedsiębiorców, wykonujących na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa. Założeniem jest, że strategiczna sieć bezpieczeństwa będzie siecią zapewniającą właściwy dla realizowanych zadań poziom bezpieczeństwa przekazywanych informacji.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Oczekiwany efekt wprowadzenia ww. narzędzi interwencji:

- Przebudowany zostanie model współpracy w ramach krajowego systemu cyberbezpieczeństwa. Sektorowe zespoły cyberbezpieczeństwa i podmioty świadczące usługi z zakresu cyberbezpieczeństwa zostaną zastąpione odpowiednio przez CSIRT sektorowe i SOC (operacyjne centra bezpieczeństwa) z tylko nieco zmienionymi zadaniami.
- Zostanie dodany nowy rodzaj podmiotu – ISAC – który umożliwi nawet niewielkim a wyspecjalizowanym podmiotom na dołączenie się do krajowego systemu cyberbezpieczeństwa.

- Utworzony zostanie Fundusz Cyberbezpieczeństwa.
- Wprowadzone zostanie świadczenie teleinformatyczne, które będzie dodatkiem do uposażenia/wynagrodzenia dla osób zajmujących się cyberbezpieczeństwem Państwa.
- Zostanie wzmocniona pozycja Pełnomocnika poprzez udostępnienie mu konkretnych uprawnień w zakresie wydawania ostrzeżeń o incydentach krytycznych wraz z zaleceniem określonych zachowań. Pełnomocnik będzie mógł również wydawać rekomendacje mające na celu wzmocnienie poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Z kolei te podmioty będą zobowiązane uwzględnić te rekomendacje podczas procesu zarządzania ryzykiem. Decyzja o zastosowaniu się do tych rekomendacji należeć będzie do tych podmiotów.
- Minister właściwy do spraw informatyzacji dzięki nowemu uprawnieniu do wydawania poleceń zabezpieczających (w ramach transparentnej procedury administracyjnej) będzie miał skuteczne narzędzie do ograniczenia skutków incydentu krytycznego w podmiotach krajowego systemu cyberbezpieczeństwa.
- Dostawcy sprzętu i oprogramowania będą mogli zostać poddani procedurze sprawdzającej pod kątem zagrożenia jakie może wywołać wykorzystywanie oferowanego przez nich konkretnego sprzętu lub oprogramowanie w podmiotach krajowego systemu cyberbezpieczeństwa. W przypadku, w którym zostaną zidentyfikowani jako źródło zagrożenia, zostaną m.in. wyłączeni z systemu zamówień publicznych w Polsce. Ponadto, podmioty krajowego systemu cyberbezpieczeństwa, których będzie obejmował zakres przedmiotowy oceny, będą musiały wycofać z użytkowania dany sprzęt lub oprogramowanie w ciągu 7 lat od wydania decyzji administracyjnej przez ministra właściwego ds. informatyzacji o ocenie ryzyka poziomu wysokiego.
- Powstanie Krajowy System Certyfikacji Cyberbezpieczeństwa w ramach, którego wydawane będą certyfikaty w zakresie cyberbezpieczeństwa.
- Minister właściwy do spraw informatyzacji będzie przygotowywać programy na podstawie, których będzie można przeprowadzać certyfikacje. Programy te będą ostatecznie przyjmowane w drodze rozporządzenia Rady Ministrów.
- Organ nadzorczy będzie przeprowadzał kontrolę w podmiotach należących do krajowego systemu certyfikacji cyberbezpieczeństwa. W zakresie certyfikatów odwołujących się do poziomu zaufania „wysoki" będzie również zatwierdzał każdy wydany certyfikat. Rozwiązanie to jest gwarantem, że ocena zgodności na najwyższy poziom bezpieczeństwa będzie przeprowadzana zgodnie z najlepszymi standardami w tej dziedzinie.
- Określone zostały procedury akredytacji jednostek oceniających zgodność oraz procedury wydawania certyfikatów
- Określone zostały obowiązki spoczywające na podmiotach krajowego systemu certyfikacji cyberbezpieczeństwa

Ustawa zagwarantuje, że zostanie uruchomiona bezpieczna sieć telekomunikacyjna wykorzystywana na potrzeby realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego przez kluczowe urzędy i podmioty działające w Rzeczypospolitej Polskiej. W tym celu zostanie powołany Operator strategicznej sieci bezpieczeństwa, który będzie wyznaczany, w drodze zarządzenia, przez Prezesa Rady Ministrów spośród podmiotów spełniających łącznie następujące warunki:

a) będących jednoosobową spółką Skarbu Państwa,
b) będących przedsiębiorcą telekomunikacyjnym,
c) posiadających infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w ust. 1,
d) posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej,
e) posiadających świadectwo bezpieczeństwa przemysłowego.

Operator te będzie świadczył usługi telekomunikacyjne, jak również inne usługi dla wskazanych w ustawie podmiotów.

Przyjęcie takiego rozwiązania zapewniłoby sprawną i zoptymalizowaną kosztowo budowę infrastruktury telekomunikacyjnej, wykorzystywanej na potrzeby realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Ponadto, skupienie realizacji szczególnie istotnych projektów w jednym miejscu przyczyni się do optymalizacji nakładów ponoszonych na nie przez Skarb Państwa oraz skrócenia czasu realizacji poszczególnych projektów. Zapewni również najwyższy poziom bezpieczeństwa dla projektów realizowanych przez Ministra Obrony Narodowej i ministra właściwego do spraw wewnętrznych, a więc dotyczących bezpieczeństwa narodowego.

Do ustawy wprowadzono możliwość pierwokupu przez Wykonawcę sieci telekomunikacyjnych pozostających we własności Skarbu Państwa lub samorządu terytorialnego.

OSSB zostanie zobowiązany do utworzenia spółki kapitałowej, która będzie pełnić funkcje operatora ogólnopolskiej hurtowej sieci, na częstotliwościach z zakresu 703 – 733 MHz oraz 758 – 788 MHz o nazwie Polskie 5G („Spółka Polskie 5G"). Kapitał zakładowy w pierwotnej wysokości będzie wynosił 1 000 000 zł (jeden miliony złotych).
Spółka Polskie 5G będzie obowiązana do:

- oferowania odpłatnych usług telekomunikacyjnych na warunkach hurtowych,
- udostępniania odpłatnie usług telekomunikacyjnych na rzecz OSSB w celu świadczenia przez niego usług telekomunikacyjnych i innych usług służących zapewnieniu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, oraz
- zapewnienia pokrycia całego terytorium kraju zasięgiem sieci hurtowej oraz zapewnienia szczególnego poziomu bezpieczeństwa w interesie publicznym w zakresie sieci oraz usług.

Prezesa UKE będzie, w drodze decyzji administracyjnej, przydzielał OSSB określony zakres częstotliwości, przeznaczony do użytkowania rządowego. Do decyzji Prezesa UKE odpowiednio będzie należało stosowanie przepisów ustawy Prawo telekomunikacyjne, dotyczących rezerwacji częstotliwości, regulujących między innymi okres, na który jest ona wydawana oraz jej treść. Jednocześnie w decyzji tej Prezes UKE obligatoryjnie określi zobowiązania pokryciowe, czyli nałożone na OSSB wymogi w zakresie pokrycia zasięgiem ruchomych sieci telekomunikacyjnych opartych o te częstotliwości.
Decyzja harmonizacyjna (Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii) w tym kontekście wyraźnie wskazuje, że nie naruszając prawa państw członkowskich do organizowania i użytkowania swojego widma radiowego do celów bezpieczeństwa publicznego oraz obronności, jeżeli została wdrożona łączność radiowa PPDR, należy stosować warunki techniczne dla bezprzewodowych usług szerokopasmowej łączności elektronicznej określonych dla aranżacji podstawowej. Państwa członkowskie mogą więc dokonać przeznaczenia określonego zasobu z pasma 700 MHz zgodnie z wytycznymi wskazanymi w Decyzji harmonizacyjnej.
Przepis ustawy wprowadza możliwość zadecydowania przez niezależnego regulatora rynku telekomunikacyjnego o szczególnym przeznaczeniu częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz. Prezes UKE może przyznać ten zakres widma przedsiębiorcy telekomunikacyjnemu lub konsorcjum przedsiębiorców telekomunikacyjnych w celu świadczenia wyłącznie usług hurtowych. Propozycja ma na celu zapewnienie Prezesowi UKE odpowiednich mechanizmów, które mogą w przyszłości doprowadzić do zintensyfikowania działań mających na celu realizację przez Rzeczpospolitą Polską celów w zakresie zapewnienia dostępu do usług szerokopasmowych każdemu obywatelowi Unii Europejskiej.
W ustawie tworzony jest państwowy fundusz celowy – Fundusz Strategicznej Sieci Bezpieczeństwa, którego dysponentem będzie minister właściwy do spraw aktywów państwowych. Przychodami Funduszu będą udziały (w wysokości 50%) we wpływach z opłat:

1) jednorazowych za rezerwacje częstotliwości w zakresie 713-733 MHz oraz 768-788 MHz,
2) jednorazowych za rezerwacje częstotliwości w zakresie 3,4-3,8 MHz,
3) rocznych za prawo do dysponowania tymin częstotliwościami, o których mowa w ustawie Prawo telekomunikacyjne.

Środki Funduszu będą przeznaczane na finansowanie wydatków związanych z:

1) budową infrastruktury na potrzeby strategicznej sieci bezpieczeństwa;
2) zapewnieniem niezawodności funkcjonalności usług świadczonych przez OSSB w ruchomej sieci telekomunikacyjnej w zakresie zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
3) udostępnieniem usług telekomunikacyjnych przez Spółkę Polskie 5G na rzecz OSSB w celu świadczenia usług przez OSSB w oparciu o częstotliwości rządowe w zakresie 703-713 MHz oraz 758-768 MHz;
4) pracami badawczo-rozwojowymi w zakresie usług świadczonych przez OSSB w ruchomej sieci telekomunikacyjnej w zakresie zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

KPRM przy projektowaniu przepisów prawa dotyczących uznania dostawców sprzętu lub oprogramowania za dostawców wysokiego ryzyka – czyli wdrożenia zaleceń z tzw. 5G Toolbox, dokonał analizy porównawczej rozwiązań prawno-organizacyjnych zaimplementowanych lub zaproponowanych mechanizmów:

- Francja:

Przepisy prawa już zostały zaimplementowane[3]. Premier Francji jest organem właściwym do wydawania zezwoleń na użytek sprzętu i oprogramowania komunikacji elektronicznej, w tym także w sprawie wykluczenia określonych dostawców oprogramowania i urządzeń. Prowadzi on również wykaz urządzeń podlegających obowiązkowi wydania dedykowanego zezwolenia, który podlega zaopiniowaniu przez Urząd Regulacji Komunikacji Elektronicznej i Poczty.
Wydanie zezwolenia na wykorzystywanie urządzeń i oprogramowania podlega ocenie pod kątem ochrony interesów bezpieczeństwa narodowego i obrony państwa. Dotyczy to urządzeń, które z uwagi na swoje funkcje mogą stwarzać zagrożenie dla trwałości, integralności, bezpieczeństwa, dostępności sieci oraz poufności przesyłu danych. Przepisy odnoszą się do operatorów komunikacji elektronicznej, którzy wykorzystują urządzenia bezpośrednio lub za pośrednictwem zewnętrznych dostawców.
Przy ocenie ryzyka brany jest pod uwagę poziom zabezpieczeń urządzeń, plany operatora rozmieszczenia i sposobu wykorzystania infrastruktury oraz fakt znajdowania się danego operatora lub jego usługodawców pod wpływem państwa trzeciego niebędącego państwem członkowskim Unii Europejskiej. Odmowa udzielenia podlega obowiązkowi uzasadnienia, chyba, że wiązałoby się to z ujawnieniem informacji niejawnych. Francja nie przewiduje żadnej formy rekompensaty dla przedsiębiorców, którzy będą musieli wycofać wskazany sprzęt lub oprogramowanie z eksploatacji.
Wydawane przez Premiera zezwolenia są ważne na okres od 3 do 8 lat – w zależności od rodzaju sprzętu lub oprogramowania. Za łamanie przepisów i warunków udzielonego zezwolenia przewidziane są sankcje karne w postaci 5 lat pozbawienia wolności lub grzywny w wysokości 300 000 euro.

- Wielka Brytania

Procedowany obecnie w Parlamencie Zjednoczonego Królestwa *Telecommunications (Security) Act 2020*[4] nowelizuje *The Communications Act 2003*. Właściwy sekretarz stanu może wydać "*designated vendor directions*" jeśli uważa, że są one niezbędne ze względu na interes bezpieczeństwa narodowego i jeśli nałożone przez ten środek wymagania są proporcjonalne. Do tych aktów muszą stosować się przedsiębiorcy telekomunikacyjni.
Designated vendor direction zawierają zakazy lub ograniczenia dotyczące używania produktów, usług dostarczanych przez dostawcę.
Designated vendor directions mają być przeglądane, co jakiś czas. Sekretarz stanu może wymagać od dostawców usług telekomunikacyjnych przygotowania i przedstawienia planu wdrożenia wymagań określonych w *designated vendor directions*. Dostawca zostaje określony w *designation notice*. Przy wydawaniu tego aktu sekretarz stanu bierze pod uwagę czynniki techniczne (jakość, niezawodność, bezpieczeństwo produktów) jak i nietechniczne (związki między dostawcą a krajem pochodzenia, tożsamość osób uczestniczących w rozwoju lub produkcji produktów).

- Finlandia

7 grudnia 2020 r. fiński parlament przyjął w nowelizacji ustawy o usługach łączności elektronicznej przepisy prawa regulujące kwestię oceny ryzyka dostawców. Organem odpowiedzialnym za ocenę sprzętu telekomunikacyjnego pod kątem zagrożenia dla bezpieczeństwa narodowego i obrony narodowej będzie Fińska Agencja Transportu i Komunikacji (The Finnish Transport and Communications Agency, FTCA). Ponadto, projekt przewiduje całkowity zakaz używania sprzętu lub oprogramowania od dostawcy wysokiego ryzyka w krytycznych częściach publicznej sieci komunikacyjnej oraz w odniesieniu do krytycznych podmiotów dla bezpieczeństwa państwa, w tym m.in. elektrowni jądrowych, portów, lotnisk oraz odpowiadających im kluczowych aktywności w sieci prywatnej podłączonej do publicznej sieci komunikacyjnej (stałe ograniczenie geograficzne)
Przed podjęciem decyzji FTCA może konsultować się z właścicielem lub operatorem sieci telekomunikacyjnej w celu umożliwienia mu usunięcia zidentyfikowanych problemów bezpieczeństwa. Jednakże, jeśli sytuacja tego wymaga (pilność

[3] Odpowiednie przepisy zawiera: *Décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article L. 34-11 du code des postes et des communications électroniques* https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039455649/.

[4] *Telecommunications (Security) Bill*, https://services.parliament.uk/bills/2019-21/telecommunicationssecuritybill.html.

sprawy), a usunięcie podatności i konsultacje z operatorem nie mogą być zrealizowane, Agencja wydaje decyzje bez konsultacji z danym podmiotem.
Organem wspierającym działalność FTCA będzie nowoutworzony organ o nazwie Rada ds. Bezpieczeństwa Sieci (Network Security Advisory Board). Rada powoływana jest przez rząd i posiada kompetencje opiniodawczo-doradcze. Wydaje zalecenia m.in. w zakresie uwzględnienia kwestii bezpieczeństwa narodowego i ochrony sieci telekomunikacyjnych, w szczególności w ich krytycznych elementach. W skład Rady wchodzą m.in. przedstawiciele ministerstw oraz przedsiębiorcy telekomunikacyjni.. FTCA ma obowiązek uwzględnić opinię wydaną przez Radę ds. Bezpieczeństwa Sieci.
Prawo przewiduje możliwość uzyskania pełnego odszkodowania za straty poniesione w związku z nakazem wycofania określonego sprzętu z użytku pod warunkiem, że sprzęt wprowadzono do użytku przed wejściem w życie znowelizowanej ustawy. Wysokość odszkodowania jest uzależniona od wyceny kosztów oraz poniesionych strat finansowych.

- Szwecja

Rozwiązania szwedzkie reguluje Ustawa o łączności elektronicznej. Organem uprawnionym do udzielania zezwoleń na użytek danego sprzętu i oprogramowania jest Krajowy Urząd Poczty i Telekomunikacji (The National Post and Telecom Authority, PTS), który ma obowiązek wystąpić o wiążącą opinię Służb Specjalnych (The Swedish Security Service) oraz Sił Zbrojnych Szwecji. Dostawcy sprzętu i oprogramowania oceniani są pod kątem zagrożenia dla bezpieczeństwa narodowego.
Podmioty ubiegające się o uzyskanie zezwolenia na użytek sprzętu i oprogramowania składając wniosek są zobowiązani odnieść się do kwestii dotyczących wpływu właścicieli przedsiębiorstwa na działalność wnioskodawcy. Ponadto oceniany jest poziom powiązań operatora z rządem lub władzami państw trzecich niebędących państwami członkowskimi Unii Europejskiej. Ocenie podlega także prawodawstwo państwa pochodzenia wnioskodawcy, szczególnie pod kątem poszanowania zasad praworządności i ochrony danych, powiązań operatora z państwami i organizacjami prowadzącymi ofensywne działania w cyberprzestrzeni wymierzone przeciwko Szwecji.
Wnioskodawca ma prawo odwołania się do Sądu Administracyjnego od wyroku którego przysługuje zaskarżenie do Sądu Apelacyjnego, który jest ostatnią instancją rozpatrującą sprawy z zakresu telekomunikacji.
Udzielone zezwolenie może być w każdym momencie wycofane, jeżeli zaistnieją przesłanki wskazujące na powstanie zagrożenia dla bezpieczeństwa państwa.

- Estonia

W 2020 roku Parlament Estonii (Riigikogu) przyjął nowelizację ustawy o komunikacji elektronicznej. Nowe przepisy upoważniają rząd do wprowadzenia obowiązku przedstawienia przez przedsiębiorstwo telekomunikacyjne szczegółowych informacji o sprzęcie i oprogramowaniu wykorzystywanych w sieciach komunikacji elektronicznej w celu zapewnienia bezpieczeństwa narodowego. Rząd otrzymał również uprawnienia do nałożenia na przedsiębiorcę telekomunikacyjnego obowiązku wystąpienia o pozwolenie na użytkowanie danego sprzętu lub oprogramowania.
Obecnie trwają prace nad rozporządzeniem określającym szczegółowe zasady uzyskiwania zezwoleń i składania sprawozdań, jak i organów odpowiadających za te działania.

- Niemcy

Organem właściwym w zakresie wyłączania komponentów producenta uznanego za dostawcę wysokiego ryzyka jest Federalne Ministerstwo Spraw Wewnętrznych, Mieszkalnictwa i Budownictwa. Ministerstwo określa także minimalne wymagania dotyczące uzyskiwania zezwoleń na użytkowanie sprzętu i oprogramowania przy infrastrukturze krytycznej w celu zapewnienia bezpieczeństwa narodowego.
Ocena dostawców odbywa się m.in. pod kątem rzetelności w wykonywaniu warunków udzielonego zezwolenia oraz wykorzystywania sprzętu i oprogramowania mogącego negatywnie wpływać na bezpieczeństwo, integralność lub działanie infrastruktury krytycznej.
Dostawcy usług telekomunikacyjnych mający siedzibę poza terytorium Niemiec zostali zobowiązani do utworzenia oddziału i punktu kontaktowego na terytorium RFN.
Federalny Urząd Bezpieczeństwa Informatycznego (Bundesamt für Sicherheit in der Informationstechnik, BSI) posiada uprawnienia do przeprowadzania kontroli bezpieczeństwa federalnych sieci komunikacyjnych i ich komponentów, jak i żądania dostępu do wszelkich danych podlegających przedmiotowi kontroli. BSI określa warunki techniczne sprzętu i oprogramowania kwalifikujące do uzyskania certyfikatów cyberbezpieczeństwa.

Dla produktów uznanych za bezpieczne wprowadzono także możliwość oznaczenia ich znakiem bezpieczeństwa informatycznego.
Za łamanie przepisów przewidziane są kary pieniężne w wysokości od 1 do 20 mln EUR lub 2-4% rocznego obrotu przedsiębiorstwa w zależności od tego, która kwota będzie wyższa.

- Słowacja

Projekt nowelizacji ustawy o cyberbezpieczeństwie zakłada nadanie szeregu nowych uprawnień Urzędowi ds. Cyberbezpieczeństwa (Úrad v oblasti kybernetickej bezpečnosti).
Urząd będzie mógł podjąć decyzję o nakazie wycofania z użytku komponentów określonego producenta przez operatora usługi kluczowej w celu zapewnienia bezpieczeństwa narodowego.
Do kompetencji Urzędu będzie także należało przyznawanie i odbieranie certyfikatów cyberbezpieczeństwa produktów, usług i procesów. Odwołanie od decyzji Urzędu będzie można wnieść w trybie określonym w kodeksie postępowania administracyjnego.
Ponadto operatorzy usług kluczowych, przedsiębiorcy i organy administracji publicznej zostaną zobowiązani do przedstawienia Urzędowi dokumentacji związanej z zapewnianiem cyberbezpieczeństwa.

- Rumunia

Projekt zmian przepisów prawa dot. bezpieczeństwa infrastruktury ICT i zasad wdrażania technologii 5G znajduje się na wczesnym etapie procesu legislacyjnego. Projekt przewiduje, że premier Rumunii po zasięgnięciu wiążącej opinii Najwyżej Rady Obrony Narodowej (CSAT) podejmuje decyzję o przyznaniu zezwolenia lub odmowie na korzystanie z technologii, sprzętu i oprogramowania ICT wykorzystywanych w sieci 5G. Ocenę dostawcy dokona się w oparciu o ryzyko dla bezpieczeństwa narodowego i obrony narodowej. Wniosek o wydanie zezwolenia na użytek sprzętu lub oprogramowania składać będzie producent w Ministerstwie Transportu, Infrastruktury i Łączności. Ministerstwo niezwłocznie przekaże wówczas wniosek do zaopiniowania przez CSAT. Premier wyda decyzję w ciągu 4 miesięcy od dnia złożenia wniosku. Decyzja o przyznaniu zezwolenia na użytek sprzętu i oprogramowania nie jest ostateczna. Po wystąpieniu zagrożeń dla bezpieczeństwa narodowego i obrony narodowej może zostać wycofana przez Premiera Rumunii na wniosek CSAT.
Do wniosku dostawca dołączyć ma list intencyjny podpisany przez przedstawiciela prawnego. Sam wniosek musi zawierać dane indentyfikacyjne wnioskodawcy, strukturę akcjonariatu i grupę kapitałową, do której należy oraz deklarację o spełnianiu następujących warunków: wnioskodawca nie podlega kontroli obcego rządu w przypadku braku niezależnego sądownictwa, ma przejrzystą strukturę akcjonariatu, nie stosował w przeszłości nieuczciwych praktyk handlowych, a ustawodawstwo w państwie pochodzenia wnioskodawcy gwarantuje przejrzystość praktyk handlowych.
Przysługuje procedura odwoławcza zgodnie z Kodeksem Postępowania Administracyjnego. Odwołania składa się do Sądu Apelacyjnego w Bukareszcie w ciągu 30 dni od opublikowania decyzji w rumuńskim Dzienniku Urzędowym, bez przeprowadzania procedury wstępnej.
Okres na wycofanie sprzętu nieposiadającego zezwolenia na użytkowanie wynosi 5 lat od momentu wejścia w życie ustawy.

Ostrzeżenia – doświadczenia z Czech

Czeska agencja ds. cyberbezpieczeństwa NUKIB na podstawie sekcji 12 (1) ustawy o cyberbezpieczeństwie[5], może wydawać ostrzeżenia do podmiotów. Ostrzeżenia wydawane są w przypadku wysokiego prawdopodobieństwa wystąpienia sytuacji kryzysowej, która może mieć krytyczne znaczenie dla bezpieczeństwa państwa. Ostrzeżenie zawiera także listę rekomendowanych działań, które podmioty powinny wdrożyć celem ograniczenia ryzyk związanych z sytuacją kryzysową. Przykłady rekomendacji: zwrócenie uwagi na określony typ cyberataków np. spear-phishingów, potrzebie zablokowania dostępu do swojej infrastruktury IT, pilnej konieczności dokonania aktualizacji oprogramowania, czy też zwrócenie szczególnej uwagi na wskazane w ostrzeżeniu domeny. Przykładem takiego ostrzeżenia jest dokument wydany 16 kwietnia 2020 r. Szefa agencji NUKIB, na podstawie analizy możliwych zagrożeń wydał ostrzeżenie dla całego państwa, ze szczególnym naciskiem na sektor ochrony zdrowia.

Certyfikacja Cyberbezpieczeństwa

[5] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) https://www.zakonyprolidi.cz/cs/2014-181.

Należy wskazać na wstępie, że inne państwa Unii Europejskiej nie implementowały jeszcze przepisów aktu o cyberbezpieczeństwie w związku z czym przeanalizowane rozwiązania dotyczą ogólnych przepisów związanych z certyfikacją w cyberbezpieczeństwie a nie modeli wdrożenia tego konkretnego aktu prawnego.

KPRM w kontekście zmian prawa w obszarze certyfikacji cyberbezpieczeństwa dokonał analizy rozwiązań przyjętych w następujących państwach:

- Francja

W ramach Francuskiej Agencji Cyberbezpieczeństwa (The National Cybersecurity Agency of France, zwana dalej ANSSI) kwestiami certyfikacji zajmuje się Narodowe Centrum Certyfikacji. Agencja ta zajmuje się również licencjonowaniem laboratoriów w tym zakresie.

Sama certyfikacja czy licencjonowanie nie podlega opłatom. Osoby wnioskujące ponoszą koszty badań laboratoryjnych ich produktów. Wynoszą one zwykle 600-700 euro na dzień a sama certyfikacja trwa ok. 25-35 dni. Podmioty obsługiwane są w kolejności złożenia wniosków co często powoduje, iż zainteresowani muszą czekać na otrzymanie usługi. Certyfikacji można dokonać również u autoryzowanych podmiotów działających na wolnym rynku.

System francuski zasadniczo różni się od przyjętego w niniejszej ustawie. Wynika to przede wszystkim z uwarunkowań instytucjonalnych. Niemiecki urząd wykonuje zadania niezwykle zbliżone do tych wynikających z implementowanego rozporządzenia jak również posiada zadania wykonywane w Polsce przez Agencję Bezpieczeństwa Wewnętrznego. W związku z tym rozwiązania te byłyby bardzo trudne do przeniesienia do polskiego porządku prawnego.

- Wielka Brytania

Przepisy prawa już zostały zaimplementowane. Narodowe Centrum Cyberbezpieczeństwa (The National Cyber Security Cente, NCSC) prowadzi wykaz dostawców wysokiego ryzyka. W celu zapewnienia bezpieczeństwa narodowego i zabezpieczenia krajowych sieci telekomunikacyjnych, NCSC na wniosek rządu wydaje rekomendacje mające na celu ograniczenie lub wyłączenie działalności podmiotu, którzy może zagrozić cyberbezpieczeństwu Wielkiej Brytanii.

- Szwecja

Kwestiami certyfikacji w Szwecji zajmuje się jedna z agencji rządowych - Swedish Defence Materiel Administration. Pobierana są liczne opłaty. Sam wniosek o certyfikację podlega bezzwrotnej opłacie, w wysokości 20 000 koron. Agencja ta zajmuje się również zamówieniami dla szwedzkich sił zbrojnych oraz rozwojem technologii na potrzeby wojska.

To sprzężenie kwestii cyberbezpieczeństwa w wymiarze cywilnym i wojskowym stanowi zasadniczą różnicę między polskim a szwedzkim systemem w tym zakresie.

- Włochy

Przyjęty we Włoszech model certyfikacji oparty jest na działaniach organów administracji publicznej. Certyfikaty wydawane są przez odpowiednią komórkę w Ministerstwie Rozwoju Gospodarczego. W związku z tym, ten rodzaj działalności organów administracji publicznej jest finansowany w całości z budżetu państwa. Równocześnie podmioty ubiegające się o certyfikat nie muszą wnosić opłat w związku z jego wydaniem.

Analiza w zakresie operatora strategicznej sieci bezpieczeństwa

W analizowanych krajach (Austria, Belgia, Finlandia, Francja, Niemcy, Węgry) udział wyspecjalizowanych jednostek państwowych lub operatorów państwowych w zarządzaniu sieciami w warstwie bezpieczeństwa oraz w warstwie aplikacyjnej jest 100-procentowy. Agendy te oraz firmy są nadzorowane albo przez ministrów bezpieczeństwa wewnętrznego (Belgia, Austria, Niemcy, Węgry) albo przez jednostki międzyresortowe podległe bezpośrednio premierowi
(Finlandia, Francja).
Warstwa szkieletowa i dystrybucyjna sieci krytycznych może być bezpośrednio lub pośrednio własnością państwa (Finlandia, Węgry, częściowo Francja i Belgia) lub może być dzierżawiona w formie usług transmisji danych lub ciemnych włókien od

kwalifikowanych operatorów komercyjnych (pozostałe analizowane kraje). Dostawcy ci są na ogół wybierani w postępowaniach zamkniętych, na podstawie specjalnych dekretów (ustaw) bądź w trybie negocjacji. Podobnie nabywane są usługi integracyjne i usługi wsparcia technicznego (maintenance sieci). Ustawy dające podstawę prawną dla pomięcia trybów konkurencyjnych powołują się artykuł 296 Traktatu UE, który zezwala krajom członkowskim na samodzielne kształtowanie polityki zakupowej w sprawach dotyczących obronności kraju.

Poniżej opisane zostaną przykłady rozwiązań z zakresu zarządzania strategicznymi z punktu widzenia państwa sieciami teleinformatycznymi i zadaniami z zakresu telekomunikacji w trzech państwa Unii Europejskiej: Finlandii, Francji i na Węgrzech.

Finlandia

W maju 1998 r. w Finlandii uruchomiono pierwszą na świecie ogólnokrajową sieć bezpieczeństwa publicznego wykorzystującą standard TETRA. Jest ona obecnie częścią zintegrowanej sieci łączności kryzysowej VIRVE. Sieć jest w całości własnością państwa, właścicielem jest istniejąca od 1992 r. grupa państwowych spółek Suomen Erillisverkot Oy (Grupa Sieci Bezpieczeństwa Państwa).

Formalnie Suomen Erillisverkot podlega bezpośrednio Kancelarii Premiera Rady Ministrów – obecnie na podstawie Rozporządzenia Rady Ministrów o polityce własności państwowej z 2011 r. oraz ustawy o bezpiecznych sieciach administracji państwowej nr 10/2015 20 .

Ustawa 10/2015 zawiera bezpośrednie umocowanie Suomen Erillisverkot lub jej spółek zależnych jako dostawców infrastruktury i usług sieciowych bezpiecznych sieci administracji państwowej Użytkownikami uprawnionymi do bezpłatnego korzystania z usług VIRVE są policja, straż pożarna, ratownictwo medyczne, siły zbrojne (dysponujące też własną infrastrukturą łączności). Należąca do grupy Suomen Erillisverkot spółka Suomen Turvallisuusverkko dostarcza usługi bezpiecznej transmisji danych dla całej administracji centralnej, a także usługi kolokacyjne oraz zarządzane usługi telekomunikacyjne.

Francja

We Francji Jednym z głównych organów wykonawczych w zakresie ochrony infrastruktury krytycznej państwa (w szerszym kontekście obronności i bezpieczeństwa) jest Agencja Narodowa Bezpieczeństwa Systemów Informacji (fr. ANSSI – Agence nationale de la sécurité des systèmes d'information). ANSSI została powołana dekretem nr 2009-834 z 7 lipca 2009 r. Dekret ten definiuje zadania ANSSI w zakresie bezpieczeństwa informacji, zapewnienia bezpiecznej łączności pomiędzy ministerstwami (Artykuł 3, tiret drugi) oraz wsparcia dla wszystkich operatorów infrastruktury krytycznej państwa, a dekret z 11 lutego 2011 r. powierza ANSSI misję ochrony wszystkich krajowych sieci informatycznych.

Innym organem podległym premierowi (w kontekście informatycznej infrastruktury krytycznej) jest powołany dekretem z 30 października 2012 r SGMAP (fr. Secrétariat général pour la modernisation de l'action publique), który jest między innymi właścicielem sieci RIE (fr. Le réseau interministériel de l'Etat), ekstranetu rządowego, której operatorem początkowo była komórka międzyministerialna DISIC a następnie agencja DINSIC (fr. Direction interministérielle du numérique et du système d'information et de communication de l'État). Zadania DINSIC definiuje rozporządzenie premiera Francji z dnia 21 września 2015r., które wskazuje między innymi zadanie operowania istniejącą już wówczas siecią RIE.

Jeśli chodzi o tryb zamawianych usług, to zgodnie z opublikowaną w 2013 r. Białą Księgą definiująca strategie bezpieczeństwa i obronności Francji, szczególnie istotne znaczenie maja mieć kwestie bezpieczeństwa sieci komunikacji elektronicznej oraz tworzącego je sprzętu.

Efektem opublikowania Białej Księgi w 2013 r. było rozszerzenie katalogu usług, które mogą być nabywane z pominięciem trybu zamówień publicznych (ustawa NR. 2015- 899 z 23 lipca 2015r), która w Art. 14, 16 definiuje explicite takie między innymi wyjątki:

- udostępnienie publicznych sieci telekomunikacyjnych (Art. 14 pkt 15);
- usługi bezpiecznej poczty elektronicznej (Art. 14 pkt 16 a)
- usługi, których realizacja wymaga zachowania poufności w interesie obronności kraju (Art. 14 pkt 11)

Ponadto ustawa ta przewiduje wyłączenia podmiotowe z prawa zamówień publicznych dla dostawców, którzy:

- są jednostkami budżetowymi, podlegającymi prawu zamówień publicznych (Art. 14 pkt 1) lub
- są jednostkami podległymi, nad którymi zamawiający sprawuje kontrolę, pod warunkiem że jednostka podległa ponad 80% swej aktywności realizuje na rzecz jednostki nadrzędnej.

Z uprawnień tych korzysta między innymi ANSSI, której zadaniem jest realizacja polityki cyberbezpieczeństwa Francji poprzez między innymi operowania rządową infrastrukturę telekomunikacyjną do łączności tajnej: ISIS. RIMBAUD i HORUS.

Ponadto funkcjonuje we Francji Dekret nr 2004-16 z 7 stycznia 2004 r. Dekret ten ustanawia możliwość pominięcia trybów konkurencyjnych w przypadku pewnych typów zamówień związanych z obronnością. Na mocy zarządzenia ministra obrony określa się kryteria kwalifikowania usługodawców – przez odniesienie do norm lub w inny sposób. Dekret ten powołuje się na

Art. 296 Traktatu UE, który daje krajom członkowskim swobodę decydowania w kwestii nabywania produktów i usług istotnych dla obronności kraju – o ile nie zaburza to konkurencji na szczeblu międzynarodowym (stosowano jej przepisy przy budowie sieci Rimbaud i przy projekcie ISIS).

Węgry

Na Węgrzech organem pełniącym szczególną rolę w powyższym systemie sieci jest NISz (węg. Nemzeti Infokommunikációs Szolgáltató Zrt.), państwowa spółka świadczącą usługi ICT dla administracji publicznej należąca do skarbu państwa i podległa MSW. Finansowanie NISz zapewniane jest przez Ministerstwo Rozwoju Narodowego (węg. NFM – Nemzeti Fejlesztési Minisztérium). Korzystanie ze wszystkich omawianych sieci jest na Węgrzech bezpłatne dla uprawnionych służb (użytkowników końcowych). Organa właścicielskie lub zarządzające danymi służbami korzystają z usług sieci na podstawie umów z NISz i z tym organem rozliczają się za usługi korzystając z własnych środków budżetowych. Szczegółowe regulacje dotyczące obecnej budowy, organizacji oraz działania infrastruktur łączności określono w rozporządzeniu RM 346/2010. (XII. 28.) o sieciach rządowej komunikacji elektronicznej (z późn. zm.).

NISz, na mocy ww. rozporządzenia, jest operatorem radiowego systemu EDR obsługującego policję, służby bezpieczeństwa wewnętrznego, służby celne i finansowe.

NISz razem z Ministerstwem Rozwoju Narodowego zarządza też siecią KözHáló, która ma dwa oddzielne segmenty Köznet (sieć dostępowa dla administracji i instytucji publicznych przeznaczoną do ogólnych, niekrytycznych celów administracyjnych) oraz Sulinet (sieć dostępowa dla szkół).

NISz zarządza również, na podstawie ww. rozporządzenia, siecią szkieletową NTG, zajmująca się m. in. transmisja danych i obsługą ruchu głosowego dla administracji publicznej.

Zadania NISz w dziedzinie teleinformatyki dla administracji centralnej wynikają z Rozporządzenia Rady Ministrów 309/2011. (XII. 23.) o centralnych usługach informatycznych i komunikacji elektronicznej. Zgodnie z załącznikiem nr 2 Rozporządzenia RM 309/2011 Rada Ministrów, Kancelaria Prezesa Rady Ministrów, MSW, Ministerstwo Zasobów Ludzkich, Ministerstwo Rolnictwa, Ministerstwo Sprawiedliwości, Ministerstwo Współpracy Gospodarczej z Zagranicą i Spraw Zagranicznych, Ministerstwo Gospodarki Narodowej, Ministerstwo Rozwoju Narodowego oraz podległa Ministerstwu Gospodarki Narodowej Naczelna Dyrekcja Zamówień Publicznych i Zaopatrzenia (KEF) obowiązane są korzystać z rozwiązań i usług teleinformatycznych opracowywanych i/lub dostarczanych przez NISz. NISz pełni też rolę urzędu certyfikującego dla usług zaufania i podpisu elektronicznego.

NISz jest również liderem lub członkiem konsorcjów realizujących programy operacyjne związane z tworzeniem i rozwojem usług elektronicznych dla administracji, przedsiębiorców i obywateli.

Konkluzja:

We wszystkich trzech omówionych wyżej krajach funkcjonują specjalne instytucje (we Francji agendy rządowe, w Finlandii i na Węgrzech spółki), które zapewniają łączność przewodową i bezprzewodową oraz transmisję danych dla administracji publicznej. W każdym z omawianych krajów istnieją akty prawne, powierzające te zadania ww. instytucjom bądź wprost, bądź tez przez szczególne wyłączenia ze stosowania przepisów dotyczących zamówień publicznych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operatorzy usług kluczowych	171	Wykaz OUK	Pozytywne. Motywujące operatorów usługi kluczowej do oddolnego wzmacniania współpracy w obszarze wymiany informacji m.in. o cyberzagrożeniach, podatnościach, czy dobrych praktykach poprzez tworzenie sformalizowanej struktury w oparciu o sprawdzoną koncepcję Centrum Wymiany Informacji i Analizy. Operatorzy usług kluczowej, w wyniku utworzenia obowiązkowych już CSIRT sektorowych, otrzymają bezpośrednie wsparcie przy reagowaniu na incydenty.
Dostawcy usług cyfrowych	34	Dane własne DC KPRM	Pozytywne. Motywujące dostawców usługi cyfrowej do oddolnego wzmacniania współpracy w obszarze wymiany informacji m.in. o cyberzagrożeniach, podatnościach, czy dobrych praktykach poprzez tworzenie sformalizowanej struktury w oparciu o sprawdzoną koncepcję Centrum Wymiany Informacji i Analizy.
Podmioty publiczne	Ok. 4000	Szacunki własne	Pozytywne. Motywujące wszystkie podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

Jednostki samorządu terytorialnego	16 województw 314 powiatów i 2 477 gmin	Dane MSWiA[6]	Pozytywne. Jednostki samorządu terytorialnego będą zobowiązane wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Jednostki samorządu terytorialnego będą obowiązane umożliwić operatorowi strategicznej sieci bezpieczeństwa umieszczenie na nieruchomości obiektów i urządzeń infrastruktury telekomunikacyjnej, w szczególności instalowanie urządzeń telekomunikacyjnych, przeprowadzanie linii kablowych pod nieruchomością, na niej lub nad nią, umieszczanie tabliczek informacyjnych o urządzeniach, a także ich eksploatację i konserwację, jeżeli nie uniemożliwi to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia wartości nieruchomości
Przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia	Ok. 100	Szacunki własne	Pozytywne. Przedsiębiorcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym	201	Rozporządzenie Rady Ministrów z dnia 3 listopada 2015 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym[7]	Pozytywne. Przedsiębiorcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Operatorzy Infrastruktury krytycznej[8]	128	OSR do projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw[9]	Pozytywne. Operatorzy infrastruktury krytycznej będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Krajowe instytucje płatnicze	38	Rejestr krajowych instytucji płatniczych[10]	Pozytywne. Krajowe instytucje płatnicze będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Kwalifikowani dostawcy usług zaufania	5	Rejestr kwalifikowanych usług zaufania[11]	Pozytywne. Dostawcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.
Niekwalifikowani dostawcy usług zaufania	10	Rejestr niekwalifikowanych dostawców usług zaufania[12]	Pozytywne. Dostawcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Ponadto, w ramach mechanizmu polecenia zabezpieczającego otrzymają jasne informacje i wytyczne ws. sprzętu lub oprogramowania, którego wykorzystywanie może mieć negatywne konsekwencje dla bezpieczeństwa.

[6] http://administracja.mswia.gov.pl/adm/baza-jst/843,Samorzad-terytorialny-w-Polsce.html.

[7] T.j. Dz.U. z 2020 r. poz. 1647.

[8] Dla czytelności przyjęto tą nazwę na określenie właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Jest to pojęcie powszechnie przyjęte w praktyce.

[9] Sejm IX kadencji, druk nr 203 http://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=203.

[10] https://e-rup.knf.gov.pl/.

[11] https://www.nccert.pl/uslugi.htm.

[12] https://www.nccert.pl/uslugiNK.htm.

Przedsiębiorcy telekomunikacyjni	4177	Rejestr przedsiębiorców telekomunikacyjnych[13]	Pozytywne. Motywujące. Wobec nich będzie mogło być skierowane ostrzeżenie i polecenie zabezpieczające. Operatora strategicznej sieci bezpieczeństwa będzie mógł się zwracać o zapewnienie odpłatnego dostępu do infrastruktury w celu świadczenia usług w strategicznej sieci bezpieczeństwa.
Narodowy Bank Polski	1	Informacja ogólnodostępna	Neutralne. Wobec Narodowego Banku Polskiego nie będą stosowane obowiązki dotyczące: -wycofania sprzętu lub oprogramowania od dostawcy wysokiego ryzyka oraz -stosowania się do polecenia zabezpieczającego.
Operator strategicznej sieci bezpieczeństwa - przedsiębiorca telekomunikacyjny, jednoosobowa spółka Skarbu Państwa	1	Wynika to z art. 76b projektu	Pozytywne. Operator będzie mógł świadczyć usługi telekomunikacyjne w ramach strategicznej sieci bezpieczeństwa.
Podmioty, którym operator strategicznej sieci bezpieczeństwa będzie świadczył usługi.	Podmioty wskazane w przypisie[14]	Wynika to z art. 76d projektu	Pozytywne. Podmioty te będą mogły korzystać z strategicznej sieci bezpieczeństwa .
Państwowe Gospodarstwo Wodne Wody Polskie	1	ustawa z dnia 20 lipca 2017 r. Prawo wodne[15]	Pozytywne. Motywujące. Włączone zostanie do krajowego systemu cyberbezpieczeństwa. Będzie zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
instytucje rozwoju z wyjątkiem Banku Gospodarstwa Krajowego	5	ustawa z dnia 4 lipca 2019 r. o systemie instytucji rozwoju[16]	Pozytywny. Motywujący. Zostaną włączone do krajowego systemu cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym. Bank Gospodarstwa Krajowego, będący instytucją rozwoju, już jest podmiotem krajowego systemu cyberbezpieczeństwa zgodnie z art. 4 pkt 10 ustawy o KSC.
Samodzielne Publiczne Zakłady Opieki Zdrowotnej	1282	Sprawozdanie o stanie Krajowego Rejestru Sądowego za sierpień 2020 r.[17]	Pozytywny. Motywujący. Włączone zostaną do krajowego systemie cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.

[13] https://bip.uke.gov.pl/rpt/.

[14] Kancelaria Prezydenta RP, Kancelaria Sejmu, Kancelaria Senatu, Kancelaria Prezesa Rady Ministrów, Biuro Bezpieczeństwa Narodowego; urzędy obsługujące organy administracji rządowej, organy jednostek samorządu terytorialnego oraz instytucjom podległym tym organom albo przez nie nadzorowanym, wykonującym zadania z zakresu ochrony bezpieczeństwa i porządku publicznego, bezpieczeństwa i obronności państwa, ochrony granicy państwa, ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa, dostaw energii, ochrony interesów Rzeczypospolitej Polskiej za granicą, ochrony zdrowia, weterynaryjnej ochrony zdrowia publicznego, nadzoru sanitarnego, ochrony środowiska, sprawiedliwości, w tym sądownictwa i prokuratury, Siły Zbrojne Rzeczypospolitej Polskiej oraz inne jednostki organizacyjne podległe lub nadzorowane przez Ministra Obrony Narodowej; instytucje wykonujące na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa

[15] Dz.U. 2021 r. poz. 624, 784, 1564 i 1641.

[16] Dz.U. 2021 r. poz. 1010.

[17] https://www.gov.pl/web/sprawiedliwosc/SprawozdaniaKRS.

Centrum Łukasiewicz	1	Informacja ogólnodostępna	Pozytywny. Motywujący. Włączone zostanie do krajowego systemu cyberbezpieczeństwa. Będzie zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
instytuty działające w ramach Sieci Badawczej Łukasiewicz	64	https://lukasiewicz.gov.pl/o-nas/grupy-badawcze/ dostęp 9.02.2021	Pozytywny. Motywujący. Włączone zostaną do krajowego systemu cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Międzynarodowe instytuty badawcze	2	Rejestr jednostek naukowych w bazie POL-on[18]	Pozytywny. Motywujący. Włączone zostaną do krajowego systemu cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Polska Akademia Umiejętności	1	Informacja ogólnodostępna	Pozytywny. Motywujący. Włączona zostanie do krajowego systemu cyberbezpieczeństwa. Zobowiązana będzie do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Polska Akademia Nauk	1	Rejestr jednostek naukowych w bazie POL-on[19]	Pozytywne. Jako podmiot publiczny będzie musiała wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Instytuty naukowe PAN	69	Rejestr jednostek naukowych w bazie POL-on[20]	Pozytywne. Jako podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Uczelnie publiczne	134	Rejestr jednostek naukowych w bazie POL-on[21]	Pozytywne. Jako podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Uczelnie niepubliczne	224	Rejestr jednostek naukowych w bazie POL-on[22]	Pozytywne. Jako podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane	412	Obwieszczenie Ministra Spraw Zagranicznych z dnia 17 sierpnia 2021 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych[23]	Jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane będą zgłaszały incydenty do CSIRT INT.
CSIRT sektorowe	7	Szacunki KPRM oparte o obecny wykaz sektorów kluczowych (załącznik 1 ustawy o ksc)	Pozytywne, Operatorzy usług kluczowych otrzymają bezpośrednie wsparcie eksperckich zespołów m.in. w obszarze obsługi incydentu, czy prowadzić dynamiczną ocenę ryzyka na rzecz operatorów. Za pośrednictwem CSIRT sektorowych będzie przekazywanych szereg istotnych informacji od operatorów usług kluczowych do CSIRT poziomu krajowego.
Potencjalne ISAC	Kilkadziesiąt podmiotów	Szacunki KPRM (obecnie w ramach Partnerstwa dla Cyberbezpieczeństwa funkcjonuje 11 podmiotów, a z kolejnymi 18 trwają ustalenia warunków współpracy)	Pozytywne. Motywujące podmioty krajowego systemu cyberbezpieczeństwa do oddolnego wzmacniania współpracy w obszarze wymiany informacji m.in. o cyberzagrożeniach, podatnościach, czy dobrych praktykach poprzez tworzenie sformalizowanej struktury w oparciu o sprawdzoną koncepcję Centrum Wymiany Informacji i Analizy. Podmioty krajowego systemu cyberbezpieczeństwa ustalą zasady współpracy oraz zakres

[18] https://polon.nauka.gov.pl/opi/aa/rejestry/nauka?execution=e1s1.
[19] https://polon.nauka.gov.pl/opi/aa/rejestry/nauka?execution=e1s1.
[20] https://bip.pan.pl/artykuly/152/rejestr-instytutow-naukowych.
[21] https://polon.nauka.gov.pl/opi/aa/rejestry/nauka?execution=e1s1.
[22] https://polon.nauka.gov.pl/opi/aa/rejestry/nauka?execution=e1s1.
[23] M.P. 2021 poz. 809.

			wymiany informacji. Co istotne, ISAC, które znajda się w wykazie prowadzonym przez ministra właściwego ds. informatyzacji będą mogły (po zawarciu porozumienia) przystąpić do systemu teleinformatycznego o którym mowa w art. 46 (zwany dalej systemem teleinformatycznym S46).
Organy właściwe do spraw cyberbezpieczeństwa	6	Informacja ogólnodostępna	Pozytywne. Motywujące organy właściwe ds. cyberbezpieczeństwa, nadzorujące kluczowe sektory gospodarki, do tworzenia sektorowych CSIRT, których zadaniem będzie bezpośrednie wsparcie operatorów usług kluczowych m.in. w reagowaniu na incydenty.
Kolegium ds. Cyberbezpieczeństwa	1	Informacja ogólnodostępna	Pozytywne. Kolegium otrzyma nowe kompetencje w postaci wydawania opinii w zakresie prowadzonej oceny ryzyka wobec danego dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Ponadto, Kolegium opiniuje i zatwierdza wydawanie ostrzeżeń i poleceń zabezpieczających.
Szef Agencji Wywiadu	1	Informacja ogólnodostępna	Pozytywne. Szef AW będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego. Szef AW będzie odpowiedzialny za utworzenie CSIRT INT, którego zadaniem będzie wsparcie w obsłudze incydentów polskich placówek zagranicznych.
Szef Centralnego Biura Antykorupcyjnego	1	Informacja ogólnodostępna	Pozytywne. Szef CBA będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Szef Służby Wywiadu Wojskowego	1	Informacja ogólnodostępna	Pozytywne. Szef SWW będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Pełnomocnik Rządu ds. Cyberbezpieczeństwa	1	Informacja ogólnodostępna	Pozytywne. Motywujące Pełnomocnika do podejmowania aktywnych działań wynikających z otrzymania nowych kompetencji do wydawania ostrzeżeń w sytuacji podejrzenia ryzyka wystąpienia incydentu krytycznego. Ponadto, wzmocniona została współpraca Pełnomocnika z zespołami CSIRT poziomu krajowego. Wiele informacji dotyczących cyberbezpieczeństwa będzie publikowane w Biuletynie Informacji Publicznej Pełnomocnika.
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Pozytywne. Minister właściwy ds. informatyzacji prowadzi wykazy ISAC oraz SOC, dzięki temu podmioty wpisane do wykazu, po zawarciu oddzielnego porozumienia z ministrem właściwym ds. informatyzacji, będą mogły przyłączyć się do z systemu teleinformatycznego S46.. Ponadto, wykazy zmobilizują ministra właściwego ds. informatyzacji do działań promujących korzyść, iż przystąpienia do współpracy ws. systemu teleinformatycznego S46.. Ponadto, minister prowadzi postępowania w sprawie uznania za dostawcę wysokiego ryzyka (po zasięgnięciu opinii Kolegium) dla dostawców sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Minister uzyska również uprawnienia kontrolne wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Będzie też prowadził postępowania administracyjne w sprawach związanych z certyfikacją np. zatwierdzał certyfikatu odnoszące się do poziomu zaufania „wysoki”.

			Będzie informował Prezesa Narodowego Banku Polskiego o wydanych decyzjach o uznaniu dostawcy za dostawcę sprzętu lub oprogramowania oraz o wydanych poleceniach zabezpieczających.
Prezes Rady Ministrów	1	Informacja ogólnodostępna	Będzie mógł wyznaczyć w drodze zarządzenia, operatora strategicznej sieci bezpieczeństwa, spośród jednoosobowych spółek Skarbu Państwa będących przedsiębiorcami telekomunikacyjnymi. Otrzyma możliwość wydania decyzji, w której będzie mógł przekazać realizowanie zadań, o których mowa w art. 26 ustawy o KSC, Ministrowi Obrony Narodowej. Decyzja będzie mogła być wydana na podstawie rekomendacji Kolegium do Spraw Cyberbezpieczeństwa.
Minister Obrony Narodowej	1	Informacja ogólnodostępna	W przypadku wydania decyzji, o której mowa w art. 67d, będzie wykonywał część zadań określonych w art. 26.
Zespoły CSIRT poziomu krajowego	3	Informacja ogólnodostępna	Pozytywne. Motywujące do podejmowania działań wzmacniających odporność systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa m.in. poprzez otrzymanie nowych kompetencji, w tym możliwość wykonywania (w porozumieniu) testów bezpieczeństwa. Ponadto, wzmocniona została współpraca zespołów CSIRT poziomu krajowego z Pełnomocnikiem.
Polskie Centrum Akredytacji	1	Informacja ogólnodostępna	Pozytywne. Polskie Centrum Akredytacji uzyska uprawnienia do prowadzenia akredytacji w nowym obszarze tematycznym.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W dniach 30.06-8.07 2020 r. przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds. Cyberbezpieczeństwa. Swoje uwagi zgłosiło Ministerstwo Obrony Narodowej, Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy i Prezes Urzędu Komunikacji Elektronicznej. Zostały również przeprowadzone konsultacje wewnątrz resortu Ministerstwa Cyfryzacji.
W wyniku zgłoszonych uwag projekt został przeredagowany i przeprowadzono drugą turę prekonsultacji w ramach zespołu doraźnego Kolegium. Powtórzono również konsultacje wewnętrzne.

W ramach konsultacji publicznych skierowano zaproszenie do przedstawienia stanowisk do 51 podmiotów na 14 dni. Jednakże, w z uwagi na prośby ze strony partnerów społecznych, Minister Cyfryzacji (pismem z 17 września 2020 r.) przedłużył czas na zgłaszanie uwag o kolejne 14 dni – łącznie na uwagi było 28 dni.

Zaproszenie w ramach konsultacji publicznych skierowano do następujących podmiotów:

Polska Izba Informatyki i Telekomunikacji; Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji; Polska Izba Komunikacji Elektronicznej; Krajowa Izba Gospodarcza; Krajowa Izba Komunikacji Ethernetowej; Krajowa Izba Gospodarki Cyfrowej; Polska Izba Radiodyfuzji Cyfrowej; Fundacja Bezpieczna Cyberprzestrzeń; Polska Izba Handlu; Polskie Towarzystwo Informatyczne; Stowarzyszenie Inżynierów Telekomunikacji; Związek Rzemiosła Polskiego; Związek Pracodawców Mediów Publicznych; Związek Pracodawców Branży Internetowej IAB Polska; Polska Rada Biznesu; Naczelna Organizacja Techniczna; Związek Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom; Izba Gospodarki Elektronicznej; Fundacja ePaństwo; Fundacja Nowoczesna Polska; Fundacja Projekt Polska; Fundacja Panoptykon; Internet Society Poland; Związek Telewizji Kablowych w Polsce Izba Gospodarcza; Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska"; Polskie Centrum Badań i Certyfikacji S.A.; Polska Organizacja Handlu i Dystrybucji; Naczelna Rada Zrzeszeń Handlu i Usług; Polska Izba Producentów Urządzeń i Usług na rzecz Kolei; Polskie Stowarzyszenie Marketingu SMB; Amerykańska Izba Handlowa; Federacja Konsumentów; Polski Związek Przemysłu Motoryzacyjnego; Ogólnopolskie Porozumienie Organizacji Radioamatorskich; Polski Związek Krótkofalowców; Business Centre Club; Konfederacja Lewiatan; Rada Dialogu Społecznego; Krajowa Izba Gospodarki Morskiej; Krajowa Izba Rozliczeniowa; Polska Wytwórnia Papierów Wartościowych; Towarzystwo Gospodarcze Polskie Elektrownie; Fundacja im. Stefana Batorego; Fundacja Instytut Mikromakro; Fundacja My Pacjenci; Fundacja Przedsiębiorców Polskich Archiwizjoner; Fundacja Pułaskiego; Stowarzyszenie Inżynierów Telekomunikacji; Sektorowa Rada ds. Kompetencji - Telekomunikacja i Cyberbezpieczeństwo;Internet Society Poland Chapter

W ramach opiniowania zaproszenie skierowano do następujących podmiotów:

Prezes Urzędu Komunikacji Elektronicznej; Prezes Urzędu Ochrony Konkurencji i Konsumentów; Prezes Urzędu Ochrony Danych Osobowych; Prezes Głównego Urzędu Statystycznego; Rzecznik Małych i Średnich Przedsiębiorców; Wojskowe Biuro Zarządzania Częstotliwościami; Komisja Nadzoru Finansowego; Rzecznik Praw Obywatelskich; Krajowa Rada Radiofonii i Telewizji; Polski Komitet Normalizacyjny; Urząd Zamówień Publicznych; Najwyższa Izba Kontroli; Agencja Bezpieczeństwa Wewnętrznego; Agencja Wywiadu; Biuro Bezpieczeństwa Narodowego; Centralne Biuro Antykorupcyjne; Służba Kontrwywiadu Wojskowego; Służba Wywiadu Wojskowego; Rządowe Centrum Bezpieczeństwa; Służba Ochrony Państwa.

Konsultacje publiczne oraz opiniowanie odbyły się w terminie od 8 września do 6 października 2020 r., przy czym przyjmowano także uwagi przesłane w późniejszym terminie, pod warunkiem zgłoszenia tego faktu opiekunowi merytorycznemu.

Do projektu ustawy w ramach konsultacji publicznych uwagi zgłosiły następujące podmioty:

Związek Banków Polskich, Santander, Narodowy Instytut Cyberbezpieczeństwa, Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM, Bank Handlowy, Q-PRO Jakub Stoparek, RFCell Technologies Sp. z.o.o., KGHM/Związek Pracodawców Polska Miedź, Stowarzyszenie Libertariańskie, SayF, Transition Software, Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o./PGNIG SA Oddział w Zielonej Górze, Izba Przemysłowo-Handlowa Polska-Azja, Huawei Polska, Business Centre Club, Digital Poland, Excogitate, Fundacja Bezpieczna Cyberprzestrzeń, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji KIGEIT, Narodowy Bank Polski, Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych, Polskie Centrum Badań i Certyfikacji, Polski Związek Pracodawców Przemysłu Farmaceutycznego, T-Mobile, Federacja Przedsiębiorców Polskich, 1Innosystems, Polska Izba Komunikacji Elektronicznej, Fabryka E-Biznesu, Krajowa Izba Gospodarki Cyfrowej DigiCom, Home.pl, Install Tech, Polska Izba Handlu, ISACA Warsaw Chapter, Krajowy Sekretariat Łączności NSZZ Solidarność, MJC Sp. z.o.o., IAB Polska, Federacja Konsumentów, Stowarzyszenie „Miasta w Internecie", Stowarzyszenie Inżynierów Telekomunikacji, Uniwersytet Jagielloński Collegium Medicum, PKP Energetyka, Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne, ISSA Polska, Związek Przedsiębiorców i Pracodawców, Krajowy Depozyt Papierów Wartościowych, Politechnika Wrocławska. Wrocławskie Centrum Sieciowo-Superkomputerowe, EXATEL, S4IT Michał Podgórski, Orange Polska, Polsko-Chińska Główna Izba Gospodarcza SinoCham, Aberit, Młodzieżowy Delegat RP przy NATO, ERSTAR, ETOB-RES, Fundacja Alatum, GBX Soft, Instytut Lema, Mobile Logic, Mobilne Miasto, Nanocoder, NeuroGames Lab, SmartWeb Media, TELDATA, TEP Doradztwo Biznesowe, TILT, Związek Cyfrowa Polska, Signum Edward Kuś Marcin Kuś, PKN Orlen, Skandynawsko-Polska Izba Gospodarcza, Liquid Systems, Instytut Staszica, Akademia Sztuki Wojennej, Krajowa Izba Komunikacji Ethernetowej, Qualitel Service, JARTEL, Izba Gospodarki Elektronicznej, Konfederacja Lewiatan, Porozumienie Zielonogórskie. Federacja Związków Pracodawców Ochrony Zdrowia

Ponadto, w trybie opiniowania opinie przedstawiły następujące podmioty:

Biuro Bezpieczeństwa Narodowego, Rzecznik Małych i Średnich Przedsiębiorców, Prezes Urzędu Komunikacji Elektronicznej, Agencja Wywiadu, Prezes Urzędu Ochrony Danych Osobowych, Komisja Nadzoru Finansowego, Najwyższa Izba Kontroli, Urząd Zamówień Publicznych, Prezes Urzędu Ochrony Konkurencji i Konsumentów, Polski Komitet Normalizacyjny, NASK-PIB.

W procedurze opiniowania i konsultacji publicznych projektu ustawy wszystkim podmiotom umożliwiono zajęcie stanowiska w sprawie projektu, a także poddano analizie przedłożone przez te podmioty uwagi.

W ramach konsultacji publicznych i opiniowania zgłoszono szereg uwag do projektu ustawy: w ramach konsultacji: 548 uwag, a w ramach opiniowania: 53 uwagi.

Ponadto, tabele zawierające stanowisko KPRM do zgłoszonych uwag opublikowano na stronie RCL, w zakładce „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

W ramach procesu konsultacji i opiniowania znaczna liczba podmiotów zwracała szczególną uwagę na kwestie dotyczące

uregulowania w przepisach prawa oceny dostawców sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa pod kątem uznania tych dostawców za dostawców wysokiego ryzyka. Wskazano na potrzebę zapewnienia transportowości procesu oceny (najlepiej w oparciu o przepisy Kodeksu postępowania administracyjnego) oraz o zapewnieniu skutecznej drogi odwoławczej od ewentualnej negatywnej decyzji.

Ponadto, zwracano uwagę o doprecyzowanie stosowania nowych instrumentów w krajowym systemie cyberbezpieczeństwa tj.: ostrzeżeń i poleceń zabezpieczających.

Wiele uwag dotyczyło także kwestii włączenia do ustawy o krajowym systemie cyberbezpieczeństwa, przepisów prawa wdrażających Europejski Kodeks Łączności Elektronicznej. Podmioty wskazywały, że kwestie wymagań bezpieczeństwa oraz zgłaszania incydentów bezpieczeństwa powinny pozostać w regulacji sektorowej, jako ma być równolegle procedowane Prawo komunikacji elektronicznej.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2021 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	**0**	**2618,867**	**108,167**	**108,167**	**108,167**	**108,167**	**108,167**	**58,167**	**58,167**	**58,167**	**58,167**	**3 392,37**
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	392,247	92,247	92,247	92,247	92,247	92,247	42,247	42,247	42,247	42,247	1 022,47
Fundusz Szerokopasmowy	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Strategicznej Sieci Bezpieczeństwa	0	2226,62	15,92	15,92	15,92	15,92	15,92	15,92	15,92	15,92	15,92	2 369,9
Wydatki ogółem	**0**	**352,486**	**167,675**	**185,398**	**182,887**	**183,366**	**188,718**	**143,950**	**155,151**	**156,739**	**150,368**	**1 866,738**
budżet państwa	0	221,493	86,683	104,406	101,895	102,374	107,726	112,958	124,159	125,747	119,376	1 206,817
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	30,993	30,992	30,992	30,992	30,992	30,992	30,992	30,992	30,992	30,992	309,921
Fundusz Szerokopasmowy		100,0	50,0	50,0	50,0	50,0	50,0	0	0	0	0	350,000
Fundusz Strategicznej Sieci Bezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**0**	**2266,381**	**-59,508**	**-77,231**	**-74,72**	**-75,199**	**-80,551**	**-85,783**	**-96,984**	**-98,572**	**-92,201**	**1 525,632**
budżet państwa	0	-221,493	-86,683	-104,406	-101,895	-102,374	-107,726	-112,958	-124,159	-125,747	-119,376	-1 206,817
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	361,254	61,255	61,255	61,255	61,255	61,255	11,255	11,255	11,255	11,255	712,549
Fundusz Szerokopasmowy	0	-100,0	-50,0	-50,0	-50,0	-50,000	-50,000	0	0	0	0	-350,000
Fundusz Strategicznej Sieci Bezpieczeństwa	0	2226,62	15,92	15,92	15,92	15 920	15 920	15 920	15 920	15 920	15 920	2 369,9
Źródła finansowania												

	Wejście w życie projektowanej regulacji będzie stanowić od 2022 r. podstawę do ubiegania się o dodatkowe środki na ten cel z budżetu państwa w części 27 –Informatyzacja. Podjęta zostanie próba sfinansowania części wydatków ze środków unijnych, w tym w ramach Krajowego Planu Odbudowy. W przypadku braku możliwości pozyskania finansowania ze środków unijnych, wydatki zostaną sfinansowane z budżetu państwa.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	**Sala dla Kolegium do spraw Cyberbezpieczeństwa.** Budynek Kancelarii Prezesa Rady Ministrów przy ul. Królewskiej 27 – miejsce urzędowania Pełnomocnika oraz Sekretarza Kolegium - nie posiada możliwości do prowadzenia spotkań o klauzuli „tajne". **Przystosowanie sali oraz zakup sprzętu na potrzeby posiedzeń Kolegium** to koszt 363 000 zł (2022 – 179 000 i 2023 – 184 000). Koszty te zostaną poniesione w ramach cz. 27 – Informatyzacja. **Wzrost kwoty dotacji podmiotowej dla Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego.** Rosnąca liczba zgłoszeń oraz potwierdzonych incydentów zgłaszanych do CSIRT NASK (60% r/r według przekazanych raportów) wymaga rozwijania kadry CSIRT NASK zarówno w obszarze nowych i obecnych kompetencji jak i w zakresie zwiększenia liczebności zasobów specjalistycznych. Wskazać należy, że w tej chwili liczba podmiotów ustawowo zobligowana do raportowania incydentów i zgłaszania osób kontaktowych do CSIRT NASK kształtuje się na poziomie ponad 60 tysięcy. Rosnąca świadomość tych podmiotów wymaga zwiększonych nakładów na utrzymywanie relacji i sprawne procedowanie spraw wynikających z ustawy. Nie bez znaczenia jest fakt iż ostatni rok wykazuje się szczególne dużą presją płacową kadry specjalistycznej, szczególnie w obszarze cyberbezpieczeństwa. Dlatego przewiduje się wzrost kwoty dotacji podmiotowej dla Naukowe i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego wynikającej z art. 26 ust. 9 ustawy o krajowym systemie cyberbezpieczeństwa. Obecnie wysokość dotacji wynosi 8,5 mln zł – ta dotacja mieści się w ramach reguły wydatkowej obecnie obowiązującej ustawy o ksc. W ustawie nowelizującej zawarta jest nowa reguła wydatkowa, w której mieścić się będzie wzrost dotacji podmiotowej dla NASK-PIB. Docelowo od 2024 r. zakłada się, że łączny koszt dotacji podmiotowej (w ramach obydwu reguł wydatkowych) wyniesie 51 mln zł rocznie. Ogółem koszty wzrostu dotacji podmiotowej dla NASK-PIB wyniosą w latach 2022-2031 374,0 mln zł Koszty te zostaną poniesione w ramach cz. 27 – Informatyzacja. **Koszty wzrostu dotacji podmiotowej dla NASK-PIB w podziale na lata w mln zł** **2022** 2023 2024 2025 2026 2027 2028 2029 2030 2031 **8,5** 25,5 42,5 42,5 42,5 42,5 42,5 42,5 42,5 42,5 **Wsparcie osobowe urzędu obsługującego ministra do spraw informatyzacji.** W związku z nowymi zadaniami ministra właściwego do spraw informatyzacji w zakresie: • prowadzenia postępowań administracyjnych w sprawie uznania za dostawcę wysokiego ryzyka; • nadzoru i kontroli nad krajowym systemem certyfikacji cyberbezpieczeństwa, przewiduje się zwiększenie zatrudnienia o 10 etatów w urzędzie obsługującym ministra. Koszty wynagrodzenia wyniosą:

- w 2022 r. 1,14 mln zł w tym:
  - pochodne w wysokości 0,19 mln zł
- od 2023 r. do 2031 r. 1,237 mln zł rocznie w tym:
  - dodatkowe wynagrodzenie roczne w wysokości 0,08 mln zł
  - pochodne w wysokości 0,2 mln zł

Ogółem ww. koszty wynagrodzenia wyniosą 12,274 mln zł.

Koszty te zostaną poniesione w ramach budżetu państwa z cz. 27 - Informatyzacja.

Prowadzenie postępowań w sprawie uznania za dostawcę wysokiego ryzyka.

Aby zapewnić efektywność postępowań administracyjnych w sprawie uznania za dostawcę wysokiego ryzyka oraz postępowań w sprawach nałożenia administracyjnych kar pieniężnych za nie wycofanie produktów ICT, usług ICT i procesów ICT dostawcy wysokiego ryzyka przewiduje się wzmocnienie urzędu obsługującego ministra do spraw informatyzacji o 3 etaty.
Koszty zatrudnienia w latach 2022 – 2031 3 osób do prowadzenia postępowań w sprawie uznania za dostawcę wysokiego ryzyka w wysokości 3,731 mln zł.

Koszty wynagrodzeń 3 stanowisk w mln zł									
2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
0,347	0,376	0,376	0,376	0,376	0,376	0,376	0,376	0,376	0,376

Utworzenie wydziału krajowego systemu certyfikacji cyberbezpieczeństwa.

W ramach przyjęcia nowych zadań w zakresie certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji konieczne jest wzmocnienie urzędu obsługującego ten organ. W celu sprawnego wykonywania nowych zadań konieczne będzie utworzenie nowego wydziału i zatrudnienie pracowników. W pierwszym roku obowiązywania nowej ustawy konieczne będzie zatrudnienie 4 osób. W związku z rozwojem rynku certyfikacji konieczne będzie również wzmocnienie nowoutworzonego wydziału w kolejnych latach – przewidujemy konieczność zatrudnienia kolejnych 3 osób w kolejnym roku. Pracownicy tworzonego wydziału będą zajmować się przede wszystkim prowadzeniem postępowań administracyjnych, analizą rynku i współpracą międzynarodową.

Koszty zatrudnienia w latach 2022 – 2031 7 nowych osób do nowego Wydziału Krajowego Systemu Certyfikacji Cyberbezpieczeństwa wyniosą w latach 2021-2031 łącznie ok. 8,543 mln zł.

Koszty wynagrodzeń 7 stanowisk w mln zł									
2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
0,794	0,861	0,861	0,861	0,861	0,861	0,861	0,861	0,861	0,861

Koszty organizacji stanowisk pracy.

Koszty organizacji stanowisk pracy dla wskazanych wyżej 10 osób wyniosą w 2022 r. łącznie 0,09 mln. Koszty te zostaną poniesione w ramach budżetu państwa z cz. 27 - Informatyzacja.

Tworzenie krajowych programów certyfikacji cyberbezpieczeństwa.

Od 2022 r. podjęte zostaną prace nad tworzeniem krajowych programów certyfikacji cyberbezpieczeństwa. W ich ramach konieczne będzie wypracowanie standardów technicznych oraz wymagań na kilka poziomów uzasadnienia zaufania, co w praktyce oznacza konieczność przygotowania

kilku szczegółowych dokumentów technicznych w ramach jednego krajowego programu certyfikacji cyberbezpieczeństwa. Zadania te będą zlecane na rynek w formie zamówienia publicznego. Ponadto krajowe programy certyfikacji cyberbezpieczeństwa będą stanowiły nowy rodzaj dokumentów technicznych, co potencjalnie wpływa na wzrost ceny. Wypracowane rozwiązania muszą też uwzględniać stan wiedzy technicznej i najlepsze praktyki w dziedzinie cyberbezpieczeństwa. Koszt obejmuje również przeniesienie majątkowych praw autorskich do wypracowanych dokumentów. Biorąc pod uwagę, że dotychczas podobne usługi związane ze wsparciem ekspertów kosztowały ok. 100 000 zł, mając równocześnie dużo mniejszy zakres czynności, przyjęto, że koszty wykonania tego zadania wyniosą 300 000 zł w 2022 r. a w kolejnych latach kwota będzie zwiększać się o 5%. Łącznie w latach 2022-2031 koszty wyniosą ok 3,778 mln zł. Koszty te zostaną poniesione w ramach cz. 27 – Informatyzacja.

Koszty umów zlecenia bądź umów o dzieło z ekspertami tworzącymi propozycje krajowych programów certyfikacji cyberbezpieczeństwa w mln zł									
2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
0,3	0,315	0,331	0,348	0,365	0,383	0,403	0,423	0,444	0,466

Utworzenie Funduszu Cyberbezpieczeństwa.

W celu finansowania zadań ustawowych zostanie utworzony Fundusz Cyberbezpieczeństwa. Będzie on państwowym funduszem celowym, a jego dysponentem będzie minister właściwy do spraw informatyzacji.

W roku utworzenia Fundusz zostanie zasilony środkami z:

- NASK-PIB (do 100 mln zł),
- Funduszu Szerokopasmowego (do 100 mln zł),
- budżetu państwa (do 150 mln zł).

W następnych pięciu latach z Funduszu Szerokopasmowego zostanie przekazane do 50 mln zł.
Przychodami Funduszu Cyberbezpieczeństwa będą:

1) dotacje z budżetu państwa;
2) wpływy z kar, o których mowa w art. 73 i 75a ustawy o krajowym systemie cyberbezpieczeństwa,;
3) 50% wpływów z opłat za prawo do wykorzystywania zasobów numeracji, o których mowa w art. 184 ust. 1 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;
4) darowizny i spadki;
5) inne przychody.

Środki z Funduszu będą przeznaczone na:

1. świadczenie teleinformatyczne, o którym mowa w art. 62a ust. 1 oraz koszty z nim związane;
2. koszty działań związanych ze zwiększeniem poziomu cyberbezpieczeństwa systemów informacyjnych, z wyjątkiem systemów, o których mowa w pkt 3;
3. koszty działań związanych ze zwiększeniem poziomu cyberbezpieczeństwa systemów infrastruktury krytycznej;
4. koszty związane z utrzymaniem i rozwojem systemu, o którym mowa w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa;
5. koszty obsługi Funduszu i koszty z nimi związane.

Świadczenie teleinformatyczne.

Szacuje się, że osób, które będą mogły otrzymać świadczenie teleinformatyczne będzie około 154. W rozporządzeniu zostaną określone są grupy osób, które będą mogły otrzymać świadczenie, w wysokości

zależnej od charakteru wykonywanych zadań. Na potrzeby wyliczeń szacunkowych przyjęto, że w pierwszej grupie będzie 38 osób ze średnim mnożnikiem 12,5. W drugiej 38 osób ze średnim mnożnikiem 9, w trzeciej zaś 78 osób ze średnim mnożnikiem 3. Przy takim założeniu, uwzględniając tzw. pochodne łączne roczne koszty świadczenia teleinformatycznego wyniosłyby:

- Dla pierwszej grupy: 13 857 000 zł
- Dla drugiej grupy: 9 977 000 zł
- Dla trzeciej grupy: 6 827 000 zł

Obsługa Funduszu Cyberbezpieczeństwa

W urzędzie obsługującym ministra właściwego do spraw informatyzacji zostaną utworzone 3 etaty do obsługi Funduszu Cyberbezpieczeństwa. Koszty te zostaną poniesione z Funduszu Cyberbezpieczeństwa.

Koszty 3 etatów do obsługi Funduszu Cyberbezpieczeństwa

2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
0	0,305	0,331	0,331	0,331	0,331	0,331	0,331	0,331	0,331	0,331

W 2022 r. koszty utworzenia stanowisk pracy wyniosą 27 000 zł.

<u>Wzrost kwoty na dotację celową na utrzymanie i rozwój systemu teleinformatycznego S46</u>

W związku z obowiązkiem korzystania przez:

- Pełnomocnika
- zespoły CSIRT poziomu krajowego
- Prezesa Urzędu Komunikacji Elektronicznej
- zespoły CSIRT sektorowe

z systemu, o którym mowa w art. 46 ustawy KSC przewidziano wzrost kwoty na dotację celową na utrzymanie i rozwój tego systemu.

Koszty wzrostu dotacji celowej zostaną poniesione z cz. 27 – Informatyzacja.

Koszty wzrostu dotacji celowej na utrzymanie i rozwój systemu teleinformatycznego S46 w podziale na lata w mln zł

2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
0	10,153	14,459	12,714	8,844	7,882	11,75	15,452	25,079	25,046	17,009

Urządzenia dla Systemów Brzegowych Uczestnika (SBU) są finansowane ze środków budżetowych. SBU są w istocie elementami systemu teleinformatycznego S46 i muszą pozostawać pod kontrolą utrzymującego system. Po stronie Uczestnika pozostaną koszty związane z utrzymywaniem łączy telekomunikacyjnych do Centrów Operacyjnych systemu teleinformatycznego S46.

Uczestnicy/Partnerzy (operatorzy usług kluczowych, dostawcy usług cyfrowych lub podmioty publiczne, którzy są zdefiniowani w ustawie o krajowym systemie cyberbezpieczeństwa) w związku z podłączeniem się do S46 będą musieli dedykować odpowiednie zasoby ludzkie do obsługi systemu. W przypadku konieczności dodatkowego finansowania zakupu SBU, Uczestnicy mogą zrezygnować z podłączenia się do systemu S46.
Centralne finansowanie SBU zapewnia interoperacyjność sprzętu, umożliwia lepsze serwisowanie, zmniejsza koszt zakupu jednostkowego sprzętu wraz z niezbędnymi licencjami, usprawnia instalację logistycznie (SBU programuje i administruje nim operator S46).

Koszty transmisji pomiędzy Centrami Operacyjnymi będą finansowane ze środków budżetowych.

Komunikacja pomiędzy Centrami Operacyjnymi jest niezbędnym elementem, mającym na celu zapewnienie wysokiej dostępności S46. Organy właściwe do spraw cyberbezpieczeństwa, uprawnione do korzystania z systemu teleinformatycznego S46, są podmiotami z sektora administracji publicznej. Zakłada się podłączanie interesariuszy ze środków przeznaczonych na utrzymanie i rozwój S46. Po stronie Organu Właściwego znajdzie się koszt utrzymywania łącza telekomunikacyjnego do Centrum Operacyjnego.

Powstanie zespół na potrzeby całościowej analizy obrazu sytuacyjnego i analizy ryzyka na poziomie kraju.

Jednym z celów wytworzenia systemu teleinformatycznego S46 jest uzyskanie całościowego obrazu sytuacyjnego i szacowania ryzyka na poziomie kraju. Przetwarzanie i analizowane informacji na tym poziomie przez poszczególne CSIRT wiązałoby się z budowaniem kompetencji w modelu wyspowym. Co więcej doświadczenie pokazuje, że poszczególne sektory niechętnie dzielą się informacjami z własnego *constituency*. Wskazuje to na potrzebę zorganizowania centralnego zespołu analityków, którzy zajmowaliby się analizą danych, ich korelacją, normalizowaniem itp. - w systemie S46, na poziomie całego Państwa.
Pożądanym byłoby, aby analitycy byli zlokalizowani w podmiocie odpowiedzialnym za utrzymanie i rozwój systemu teleinformatycznego S46.

Liczba dołączanych SBU w ciągu roku.

Liczba dołączanych SBU wpływa na odwzorowanie sieci powiązań pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa, a zatem na odwzorowanie rzeczywistego poziomu cyberbezpieczeństwa w Polsce. Założono harmonogram podłączeń, w ramach którego do maksymalnie 2023 roku będą dołączone wszystkie podmioty KSC, a następnie będą podłączane jedynie instytucje nowe lub realizujące nowe lub zmodyfikowane przedsięwzięcia, gdy zmiana powoduje, że spełniają one kryteria podłączenia do systemu teleinformatycznego S46.
Szczegółowe wyliczenia wzrostu kwoty na dotację celową na utrzymanie i rozwój systemu teleinformatycznego S46 zawiera załącznik nr 2 do OSR.

Podłączenie Rządowego Centrum Bezpieczeństwa do systemu teleinformatycznego S46.

Koszty podłączenia Rządowego Centrum Bezpieczeństwa w 2021 r. do systemu teleinformatycznego S46 szacuje się na 20 000 zł. Są to koszty jednorazowe – zakupu sprzętu komputerowego oraz zapory sieciowej.
Zgodnie z art. 11 ust. 1 i 1a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[24] Rządowe Centrum Bezpieczeństwa obsługuje Rządowy Zespół Zarządzania Kryzysowego oraz Zespół do spraw incydentów krytycznych. Obydwa wymienione zespoły otrzymają nowe zadania w nowelizacji, które uzasadniają konieczność podłączenia Rządowego Centrum Bezpieczeństwa do systemu teleinformatycznego S46:

- Rządowy Zespół Zarządzania Kryzysowego będzie mógł wydać opinię, na podstawie której Prezes Rady Ministrów zobowiąże Ministra Obrony Narodowej o udzielenia wsparcia CSIRT koordynującemu obsługę incydentu krytycznego przez właściwe jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej
- Zespół do spraw incydentów krytycznych będzie dokonywał analizy uzasadniającej wydanie ostrzeżenia i polecenia zabezpieczającego.

[24] Dz.U. z 2020 r. poz. 1856, z 2021 poz. 159

Budowa CSIRT sektorowych.

Budowa 7 zespołów CSIRT sektorowych będzie kosztownym przedsięwzięciem, które pozwoli zapełnić lukę w reagowaniu na incydenty w najbardziej narażonych sektorach gospodarki, w których incydenty mogą mieć katastrofalne skutki. W skład usług oferowanych przez CSIRT sektorowy będą usługi tzw. CERT (analityczne) oraz SOC (reagowania na incydenty).

Koszty budowy i funkcjonowania CSIRT sektorowych w latach 2021-2031 wyniosą 449,758 mln zł, w tym:

- Koszty utrzymania w latach 2021-2031 365,73 mln zł.

  Koszty te zostaną poniesione w ramach budżetu państwa (w tym celu zostanie utworzona rezerwa celowa w cz. 83 – Rezerwy celowe). Jednocześnie będą podejmowane działania w celu sfinansowania tych wydatków ze źródeł innych niż budżet państwa.

- Koszty zakupu sprzętu i licencji na oprogramowanie w 2022 r. w wysokości 18,396 mln zł. Koszty aktualizacji i wymiany sprzętu i oprogramowania w latach 2023-2031 w wysokości ok. 65,632 mln zł.
  Koszty te zostaną poniesione z innych źródeł – w tym ze środków europejskich np. Krajowego Planu Odbudowy (do 2026 r.). W przypadku niemożliwości uzyskania środków z innych źródeł wydatki te zostaną poniesione z budżetu państwa z rezerwy celowej.

Koszty budowy i funkcjonowania CSIRT sektorowych w podziale na lata w mln zł.									
2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
44,164	39,083	41,382	42,548	43,785	45,058	46,37	47,72	49,11	50,538

Do obliczeń przyjęto utworzenie trzech rodzajów CSIRT sektorowych, w zależności od liczby operatorów usług kluczowych w danym sektorze i poziomu skomplikowania systemów informacyjnych w sektorze. Czasochłonność usług analitycznych w CSIRT sektorowych kształtuje się następująco:

Rodzaj CSIRT	**Średnia liczba roboczodni na miesiąc**	**Koszt roczny w zł**	**Sektory, w których zostaną utworzone CSIRT sektorowe danego rodzaju**
Mały CSIRT	50	594 000	Infrastruktura cyfrowa
			Zaopatrzenie w wodę i jej dystrybucja
Średni CSIRT	81	962 280	Transport wodny
			Transport lądowy i powietrzny
Duży CSIRT	111	1 318 680	Energia
			Bankowość i infrastruktura rynków cyfrowych
			Ochrona zdrowia

Załącznik nr 1 do OSR zawiera spis usług analitycznych realizowanych w ramach CSIRT sektorowego. Obliczenia czasochłonności poszczególnych zadań dokonano we współpracy z Fundacją Bezpieczeństwa Cyberprzestrzeń.

Na potrzeby obliczeń przyjęto, że specjaliści w CSIRT sektorowych będą otrzymywać wynagrodzenie odpowiadające stawkom rynkowym na podobnych stanowiskach, tj. w wysokości 18 000 zł brutto m/c. Kształtując wysokość wynagrodzenia oparto się na analizie raportów przygotowywanych cyklicznie przez niezależne podmioty, takie jak np. Hays Poland, dotyczących wynagrodzeń na rynku, w szczególności rynku IT. Pod uwagę wzięto takie stanowiska, jak np. konsultant do spraw bezpieczeństwa IT, specjalista ds. bezpieczeństwa aplikacji, specjalista ds. bezpieczeństwa infrastruktury IT, funkcjonujące w dużych organizacjach/przedsiębiorstwach. Wynagrodzenia te wynosiły od 14.000 zł do 25.000 zł.

Usługi SOC w ramach CSIRT sektorowego zakładają stopniowe budowanie trzech linii wsparcia (od 14 pracowników w pierwszym roku działania do 21 pracowników w trzecim):

SOC – etaty				**2022**		**2023**		**2024**
Typ stanowiska	**Koszt miesięczny**		**FTE[25)]**	**Roczny budżet**	**FTE**	**Roczny budżet**	**FTE**	**Roczny budżet**
Operator I linii		12 000	10	1 467 360	15	2 249 463	15	2 310 198
Analityk II linii		16 000	2	391 296	2	399 905	3	591 552
Ekspert III linii	Etatowy	20 000	1	244 560	2	499 881	2	513 377
	Koszty zewnętrzne:	20 000	-	244 560	-	249 940	-	256 689
Administrator SOC		15 000	1	183 420	1	187 455	1	192 517
SUMA		83 000	14	2 531 196	20	3 586 644	21	3 864 333

Źródło: analizy własne DC KPRM.
Powyższe wyliczenia uwzględniają wskaźniki makroekonomiczne MF.

Do kosztów działania usług SOC w ramach CSIRT sektorowych należy doliczyć koszty administracyjne i sprzętu (ok. 3 mln zł w pierwszym roku i potem ok. 30% rocznie na aktualizację i wymianę sprzętu). Koszty utworzenia 6 CSIRT sektorowych obejmują koszty zakupu sprzętu i licencji na oprogramowanie. Koszty funkcjonowania 7 CSIRT sektorowych obejmują koszty aktualizacji i wymiany sprzętu. Koszty zakupu sprzętu pierwszego wyposażenia zostaną poniesione ze środków rezerwy celowej.

Podłączenie CSIRT sektorowych do S46.

Od 2022 r. miesięczny koszt utrzymania łączy niezbędnych do korzystania z systemu S46 szacuje się na ok. 2 000 zł na jeden CSIRT sektorowych, co daje ok. 24 000 zł rocznie.

Koszty podłączenia CSIRT sektorowych do S46 w zł w 2022 r.		
Okres	**1 CSIRT sektorowy**	**7 CSIRT sektorowych**
Miesięczny	2 000	24 000

[25]) FTE – Full Time Equivalent.

Roczny	24 000	168 000

CSIRT INT
Ustawa przewiduje powstanie CSIRT INT prowadzonego przez Szefa Agencji Wywiadu. Będzie to CSIRT dedykowany dla jednostek organizacyjnych podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych.
Koszty jego budowy i funkcjonowania zostaną sfinansowane z cz. 59 budżetu państwa – Agencja Wywiadu.

Koszty budowy i funkcjonowania CSIRT INT w podziale na lata w mln zł.									
2022	2023	2024	2025	2026	2027	2028	2029	2030	2031
6,966	5,905	6,242	6,418	6,605	6,798	6,996	7,200	7,410	7,626

Powstanie strategicznej sieci bezpieczeństwa i wyznaczenie jej Operatora.

Oszacowanie skutków finansowych dla budżetu państwa w zakresie korzystania przez najważniejsze urzędy w państwie oraz służby specjalne czy też służby bezpieczeństwa i porządku publicznego, a także ochrony granic, ochronę zdrowia z usług telekomunikacyjnych świadczonych przez operatora strategicznej sieci bezpieczeństwa nie jest możliwe do oszacowania na tym etapie.
Miemierzalnym skutkiem dla budżetu państwa jest zapewnienie takiego funkcjonowania bezpiecznego ekosystemu sieci telekomunikacyjnej dla najważniejszych osób, urzędów i służb w państwie, który do minimum ograniczy incydenty bezpieczeństwa i konieczność reagowania na nie.

Spółka Polskie 5G.

W projekcie ustawy przewidziano, że OSSB utworzy spółkę kapitałową która będzie pełnić funkcję operatora ogólnopolskiej hurtowej sieci o nazwie Polskie 5G, zwaną dalej: „Spółka Polskie 5G".

Udziały w Spółce Polskie 5G obejmują:

1) 26 % - Operator sieci strategicznej bezpieczeństwa w zamian za wkłady pieniężne;
2) 26 % - Polski Fundusz Rozwoju S.A. lub fundusze, których częścią portfela inwestycyjnego zarządza Polski Fundusz Rozwoju S.A. w przypadku nieobjęcia w całości lub w części 26% udziałów albo akcji przez Polski Fundusz Rozwoju S.A. lub fundusze, których częścią portfela inwestycyjnego zarządza Polski Fundusz Rozwoju S.A. nieobjęte udziały albo akcje, o których mowa powyżej obejmie operator strategicznej sieci bezpieczeństwa. Wskazane udziały albo akcje zostaną objęte za wkłady pieniężne.
3) 48% - przedsiębiorca telekomunikacyjny, któremu zostaną przyznane częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz, lub jeżeli częstotliwości te zostaną przyznane konsorcjum przedsiębiorców telekomunikacyjnych – każdemu z nich w częściach równych w zamian za wkłady pieniężne, po zakończeniu przetargu, o którym mowa art. 76p ust. 1.

Fundusz Strategicznej Sieci Bezpieczeństwa.

Projekt ustawy przewiduje utworzenie Funduszu Strategicznej Sieci Bezpieczeństwa, jako państwowego funduszu celowego, którego dysponentem będzie minister właściwy do spraw aktywów państwowych.
Przychodami Funduszu będą:

1) 50% opłat jednorazowych za rezerwacje częstotliwości w zakresie 713-733 MHz oraz 768-788 MHz,
2) 50% opłat jednorazowych za rezerwacje częstotliwości w zakresie 3,4-3,8 MHz,
3) 50% opłat rocznych za prawo do dysponowania tymi częstotliwościami, o których mowa w

ustawie Prawo telekomunikacyjne.

Środki Funduszu będą przeznaczane na finansowanie wydatków związanych z:

1) budową infrastruktury na potrzeby strategicznej sieci bezpieczeństwa;
2) zapewnieniem niezawodności funkcjonalności usług świadczonych przez OSSB w ruchomej sieci telekomunikacyjnej w zakresie zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
3) udostępnieniem usług telekomunikacyjnych przez Spółkę Polskie 5G na rzecz OSSB w celu świadczenia usług przez OSSB w oparciu o częstotliwości rządowe w zakresie 703-713 MHz oraz 758-768 MHz;
4) pracami badawczo-rozwojowymi w zakresie usług świadczonych przez OSSB w ruchomej sieci telekomunikacyjnej w zakresie zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Wpływ projektu ustawy na jednostki samorządu terytorialnego.

Wprowadzone przepisy w zakresie certyfikacji zapewnią większą dostępność rozwiązań technicznych zapewniających bezpieczeństwo indywidualnym użytkownikom

Jednostki samorządu terytorialnego są zobowiązane na podstawie paragrafu 20 rozporządzenia o Krajowych Ramach Interoperacyjności[26)] do przeprowadzania zarządzania ryzykiem. Wobec tego będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Natomiast decyzja o uwzględnieniu tych środków będzie należała wyłącznie do nich.

Jednostki samorządu terytorialnego będą obowiązane umożliwić operatorowi strategicznej sieci bezpieczeństwa umieszczenie na nieruchomości obiektów i urządzeń infrastruktury telekomunikacyjnej, w szczególności instalowanie urządzeń telekomunikacyjnych, przeprowadzanie linii kablowych pod nieruchomością, na niej lub nad nią, umieszczanie tabliczek informacyjnych o urządzeniach, a także ich eksploatację i konserwację, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia wartości nieruchomości. Jednostce samorządu terytorialnego zostanie zwrócona część kosztów związanych z zapewnieniem dostępu.

Wpływ finansowy projektu ustawy na jednostki samorządu terytorialnego jest niemożliwy do oszacowania.

Do wszystkich kosztów dodano spodziewany wzrost cen, zgodnie z tabelami makroekonomicznymi MF.

6. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki									
Czas w latach od wejścia w życie zmian			0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym		duże przedsiębiorstwa	-	10,625	6,63	6,63	6,63	6,63	37,145
		sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-

[26)] Rozporządzenie 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. t.j. Dz.U. z 2017 r. poz. 2247

(w mln zł, ceny stałe z 2021 r.)		rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
W ujęciu niepieniężnym		duże przedsiębiorstwa	Zmiany w ustawie o krajowym systemie cyberbezpieczeństwa spowodują konieczność wypracowania przez operatorów usług kluczowych procedur kontaktu z zespołami CSIRT sektorowymi. Operatorzy usług kluczowych będą zobowiązani korzystać z systemu S46 od 1 stycznia 2023 r. co spowoduje konieczność poniesienia kosztów jednorazowych (zakup sprzętu, oprogramowania i łączy) oraz stałe koszty abonamentu łączy i energii. W ramach Krajowego Planu Odbudowy oraz funduszu REACT-EU planowane jest sfinansowanie podłączenia niektórych podmiotów, w tym operatorów usług kluczowych, do systemu S46. Dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się podmiotami prowadzącymi SOC na rzecz operatorów usług kluczowych. Zmieni się zakres obowiązków SOC w stosunku do poprzednich przepisów ustawowych. Z chwilą wejścia w życie nowelizacji SOC będą wdrażały zabezpieczenia na podstawie przeprowadzonego szacowania ryzyka. Oznaczać to będzie, że wprowadzone środki techniczne i organizacyjne będą mogły różnić się od dotychczas wprowadzonych, ponieważ to SOC będzie o nich decydował. Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych czy przedsiębiorcy telekomunikacyjni (będący dużymi przedsiębiorstwami) w zależności od decyzji ministra właściwego ds. informatyzacji w zakresie oceny ryzyka będą musiały wycofać dany sprzęt lub oprogramowanie z użycia w ciągu 7 lat (dostawcy wysokiego ryzyka). Podkreślenia wymaga, że wycofaniu będą podlegały produkty, usługi, procesy określone w decyzji – a więc nie wszystkie produkty (usługi, procesy) oferowane przez dostawcę wysokiego ryzyka. Natomiast przedsiębiorcy telekomunikacyjni, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesy ICT wskazanych w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa Państwa funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku. Podmioty zobowiązane do wycofania produktów, usług i procesów pochodzących od dostawcy wysokiego ryzyka nie będą mogły ich zamawiać poprzez Prawo zamówień publicznych, jeżeli do nich stosuje się ta ustawa. Ponadto, w wyniku wydania decyzji administracyjnej ws. polecenia administracyjnego, podmioty krajowego systemu cyberbezpieczeństwa,							

			których będzie dotyczyła ta decyzja m.in. zakazującej korzystania z określonego oprogramowania, które zostało wskazane jako stanowiące zagrożenie dla wystąpienia incydentu krytycznego. Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. Nowelizacja wprowadza kary za niedostosowanie się do obowiązku wycofania produktów ICT, usług ICT i procesów ICT dostawcy wysokiego ryzyka a także za niedostosowanie się do obowiązku wykonania określonego zachowania zawartym w poleceniu zabezpieczającym. Kary te wyniosą do 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Oczywiście znajdą tutaj zastosowanie przepisy dotyczące administracyjnych kar pieniężnych z Kodeksu postępowania administracyjnego. Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. W związku z działalnością operatora strategicznej sieci bezpieczeństwa przedsiębiorcy telekomunikacyjni udostępniają swoją infrastrukturę na zasadach odpłatności.
		sektor mikro-, małych i średnich przedsiębiorstw	Zmiany w ustawie o krajowym systemie cyberbezpieczeństwa spowodują konieczność wypracowania przez operatorów usług kluczowych procedur kontaktu z zespołami CSIRT sektorowymi Dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się podmiotami prowadzącymi SOC na rzecz operatorów usług kluczowych. Zmieni się zakres obowiązków SOC w stosunku do poprzednich przepisów ustawowych. Z chwilą wejścia w życie nowelizacji SOC będą wdrażały zabezpieczenia na podstawie przeprowadzonego szacowania ryzyka. Oznaczać to będzie, że wprowadzone środki techniczne i organizacyjne będą mogły różnić się od dotychczas wprowadzonych, ponieważ to SOC będzie o nich decydował. Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych w zależności od decyzji ministra właściwego ds. informatyzacji w zakresie oceny ryzyka będą musiały wycofać dany sprzęt lub oprogramowanie z użycia w ciągu 7 lat (dostawcy wysokiego ryzyka). Obowiązek wycofania produktów, usług i procesów dostawcy wysokiego ryzyka będzie dotyczył tych mikro-, małych i średnich przedsiębiorców telekomunikacyjnych, którzy sporządzają plany działań w sytuacji szczególnego zagrożenia.

			Ponadto, w wyniku wydania decyzji administracyjnej ws. polecenia administracyjnego, podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni (wszyscy), operatorzy infrastruktury krytycznej, przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym, dostawcy usług zaufania, których będzie dotyczyła ta decyzja m.in. zakazująca korzystania z określonego oprogramowania, które zostało wskazane jako stanowiące zagrożenie dla wystąpienia incydentu krytycznego. Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. W związku z działalnością operatora strategicznej sieci bezpieczeństwa przedsiębiorcy telekomunikacyjni udostępniają swoją infrastrukturę na zasadach odpłatności.
		rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje ustawowe przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększą pewność ciągłości usług. Część kosztów wypełnienia obowiązków ustawowych, w przypadku niektórych sektorów, może przełożyć się na wyższy koszt usługi dla odbiorcy końcowego.
Niemierzalne		Koszty związane z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka	Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni, operatorzy infrastruktury krytycznej oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo obronnym w związku z wycofaniem produktów, usług i procesów pochodzących od dostawców wysokiego ryzyka ponieważ nie można w tej chwili przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji i w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu. Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
		Koszty związane z wykonaniem polecenia zabezpieczającego	Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania polecenia zabezpieczającego w formie decyzji administracyjnej. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni, operatorzy infrastruktury krytycznej oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, dostawcy usług zaufania, krajowe instytucje płatnicze ponieważ polecenie zabezpieczające będzie wydawane po wystąpieniu incydentu krytycznego.

			Będzie wskazywało obowiązek zachowania adekwatny do charakteru incydentu krytycznego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń			Wpływ na konkurencyjność gospodarki i przedsiębiorczość będzie różnił się w zależności od typu podmiotu (operator usług kluczowych, dostawca usług cyfrowych, SOC, przedsiębiorców telekomunikacyjnych) i sektora.

7. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:
Ustawa spowoduje zmniejszenie w niektórych obszarach (SOC) obciążeń regulacyjnych, za to wprowadzi nowe – dla ISAC, oraz dostawców sprzętu lub oprogramowania.

Ustawa celowo nie nakłada wiele obowiązków na ISAC, aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.

Operatorzy usług kluczowych będą zobowiązani do korzystania z systemu S46 od 1 stycznia 2023 r.

Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa.
Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych w zależności od decyzji ministra właściwego ds. informatyzacji w zakresie oceny ryzyka będą musiały wycofać dany sprzęt lub oprogramowanie z użycia w ciągu 7 lat (dostawcy wysokiego ryzyka).

Podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni, operatorzy infrastruktury krytycznej oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, dostawcy usług zaufania, krajowe instytucje płatnicze będą zobowiązani do polecenia zabezpieczającego, jeżeli zostanie wydane.

Dobrowolny charakter certyfikacji sprawia, że nie dojdzie do zmiany obciążeń regulacyjnych spoczywających na przedsiębiorcach. Uczestnicy krajowego systemu certyfikacji cyberbezpieczeństwa będą musieli stosować przepisy niniejszej ustawy związane z kontrolą zarówno ze strony Polskiego Centrum Akredytacji jak i ministra właściwego do spraw informatyzacji. Udział w tym systemie jest jednak całkowicie dobrowolny.

8. Wpływ na rynek pracy

Sektor cyberbezpieczeństwa jest jednym z najbardziej dynamicznych sektorów gospodarki. W I kwartale 2019 roku odnotował on wzrost o 14,2 %. Cyberprzestępstwa wskazywane są jako jedne z pięciu najistotniejszych zagrożeń dla firm obok m.in. katastrof naturalnych. Na tak szybko zmieniającym się rynku certyfikaty w zakresie cyberbezpieczeństwa będą cenną pomocą, co do wyboru określonych produktów ICT. Przyczyni się to do większego wykorzystania bezpiecznych rozwiązań w sektorze przedsiębiorstw.

Projekt wygeneruje konieczność zatrudnienia wysoko wykwalifikowanych specjalistów zajmujących się cyberbezpieczeństwem a także przekwalifikowania dotychczas posiadanej kadry. Ponadto, pojawi się okazja do rekwalifikacji kadr oraz systemowego podnoszenia kompetencji i wiedzy osób zatrudnionych w podmiotach krajowego systemu cyberbezpieczeństwa.

9. Wpływ na pozostałe obszary

☐ środowisko naturalne ☒ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☒ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Ustawa zwiększy poziom bezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, w tym spółek Skarbu Państwa i jednostek samorządu terytorialnego. Projekt spełnia wymagania interoperacyjności, czyli zdolność systemów teleinformatycznych do efektywnej współpracy w celu zapewnienia wzajemnego dostępu użytkowników do usług świadczonych w tych sieciach. Projekt spełnia również wymogi neutralności technologicznej, wykorzystania danych z rejestrów publicznych oraz ochrony danych osobowych.

10. Planowane wykonanie przepisów aktu prawnego

Ustawa wejdzie w życie po upływie 30 dni od ogłoszenia.

Z chwilą wejścia w życie ustawy:

1. wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo powołane w ramach operatora usługi kluczowej staną się SOC powołanymi w ramach operatora usługi kluczowej;
2. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę staną się podmiotami prowadzącymi SOC na rzecz operatora usługi kluczowej;
3. sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy w brzmieniu dotychczasowym stanie się CSIRT sektorowym.
4. Podmioty publiczne wyznaczą osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.
5. Organy właściwe do spraw cyberbezpieczeństwa będą miały 18 miesięcy na ustanowienie CSIRT sektorowego.
6. Operatorzy usług kluczowych będą zobowiązani do korzystania z systemu S46 od 1 stycznia 2023 r.
7. Wyznaczenia Operatora strategicznej sieci bezpieczeństwa oraz powołanie Spółki Polskie 5G.

Pierwszym krokiem jest stworzenie jednolitych procedur akredytacji i certyfikacji na potrzeby cyberbezpieczeństwa. Równocześnie utworzony zostanie organ nadzoru, który będzie monitorował rozwój rynku certyfikacji. Odpowiednie działania zostaną podjęte w KPRM. Zatrudnione zostaną dodatkowe osoby, które będą prowadziły postępowania administracyjne oraz przeprowadzały kontrole zgodnie z niniejszą ustawą. Działania te zostaną rozpoczęte w 2021 roku, a zgodnie z przewidywaniami komórka organizacyjna utworzona do ww. zadania osiągnie pełną skład osobowy w 2022 roku.
Przyznanie uprawnień akredytacyjnych, w tym zakresie, Polskiemu Centrum Akredytacji pozwoli w możliwie krótkim horyzoncie czasowym rozpocząć akredytację jednostek certyfikacyjnym i jednostek oceniających zgodność.

Organ nadzoru będzie również w stanie określić czy istnieje potrzeba wprowadzenia krajowych programów certyfikacyjnych. Początkowo certyfikacja odbywać się będzie w ramach europejskich programów certyfikacji.

Szef Agencji Wywiadu będzie zobowiązany utworzyć CSIRT INT po wejściu w życie ustawy.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zastosowane będą następujące mierniki:
1.Liczba ISAC wpisanych do wykazu
2.Liczba powstałych CSIRT sektorowych
3.Liczba wydanych ostrzeżeń
4.Liczba akredytowanych jednostek oceniających zgodność
5.Liczba wydanych certyfikatów i wystawionych deklaracji zgodności

Ewaluacja nastąpi w dwa lata po wejściu ustawy w życie, a następnie będzie prowadzona cyklicznie, co dwa lata.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

1. Spis usług analitycznych realizowanych w ramach CSIRT sektorowego
2. Wyliczenia wzrostu kwoty na dotację celową na utrzymanie i rozwój systemu teleinformatycznego S46.

Załącznik nr 1 do OSR

1. USŁUGA – ANALIZA ARTEFAKTÓW.	
OPIS USŁUGI	**Roboczodni**
Usługa związana ze zrozumieniem możliwości i celów działania znalezionych śladów/próbek (np. złośliwego oprogramowania, exploitów, spamu i plików konfiguracyjnych), a także sposobu ich dostarczenia, wykrywania i neutralizacji.	3-7 roboczodni
2. USŁUGA – ANALIZA POWŁAMANIOWA (INFORMATYKA ŚLEDCZA)	
OPIS USŁUGI	**Roboczodni**
Usługi obejmujące analizę danych z systemów, sieci, pamięci cyfrowych i nośników wymiennych w celu lepszego zrozumienia sposobu zapobiegania, wykrywania i/lub neutralizacji podobnych lub powiązanych incydentów. Usługi te mogą dostarczać informacji do opinii prawnych, kryminalistycznych, przeglądów zgodności lub innych przeglądów informacji historycznych.	2-6 roboczodni
3. USŁUGA – ANALIZA PODATNOŚCI	
OPIS USŁUGI	**Roboczodni**
Usługi świadczone w celu lepszego zrozumienia luk w zabezpieczeniach, które były przyczyną incydentów.	4-8 roboczodni
4. USŁUGA – ROZWÓJ ORAZ ZARZĄDZANIE ŹRÓDŁAMI I DANYMI THREAT INTELLIGENCE	
OPIS USŁUGI	**Roboczodni**
Usługi świadczone na rzecz wewnętrznego lub zewnętrznego constituency w celu rozwoju i koordynowania zewnętrznych źródeł informacji dotyczących cyberzagrożeń. Usługi mogą obejmować analizę, rozwój, dystrybucję i zarządzanie informacjami o bezpieczeństwie. Dotyczą wskaźników kompromitacji, warunków logicznych detekcji, takich jak reguły i sygnatury antymalware oraz taktyki, techniki i procedury przeciwników. Usługi te zależą od działań związanych z wymianą informacji, które są zdefiniowane w obszarze usługowym numer 5 "Komunikacja".	15-20 roboczodni
5. USŁUGA – PODNOSZENIE ŚWIADOMOŚCI O ZAGROŻENIACH	
OPIS USŁUGI	**Roboczodni**
Usługi mające na celu podnoszenie świadomości o cyberzagrożeniach oraz podniesienie kompetencji w zakresie obrony przed zagrożeniami u interesariuszy.	8-15 roboczodni
6. USŁUGA – DORADZTWO W ZAKRESIE POLITYK I STRATEGII CYBERBEZPIECZEŃSTWA.	
OPIS USŁUGI	**Roboczodni**
Usługa polegająca na Konsultacjach w dziedzinie polityk bezpieczeństwa, również doradzanie *constituency* w zakresie prawnych aspektów reagowania na incydenty.	1-5 roboczodni
7. USŁUGA - DZIELENIE SIĘ INFORMACJĄ I UPUBLICZNIANIE JEJ.	
OPIS USŁUGI	**Roboczodni**
Usługa dotycząca szerokiej komunikacji, uwzględniającej powiadomienia dla *constituency*, w celu poprawy jakości procesów biznesowych. Niektóre z przykładów to komunikaty dotyczące szkoleń, wydarzeń, nowych polityk i procedur.	1-5 roboczodni
8. USŁUGA – SZKOLENIA I EDUKACJA.	
OPIS USŁUGI	**Roboczodni**
Zdolność do realizacji określonych działań jest istotą usług CSIRT, osiąganie zdolności oznacza również szkolenia i edukację odbiorców usług CSIRT oraz samego CSIRT w tematach związanych z cyberbezpieczeństwem, zabezpieczeniem informacji i reagowaniem na incydenty. Kompetencje oznaczają zdolność do realizacji działań na pewnym poziomie dojrzałości.	2-5 roboczodni

9. USŁUGA – ORGANIZACJA ĆWICZEŃ.	
OPIS USŁUGI	**Roboczodni**
Usługi oferowane przez organizację na rzecz przedstawicieli *constituency* wspierające przygotowanie, przeprowadzenie i ocenę ćwiczeń w cyberprzestrzeni, mających na celu szkolenie i/lub ocenę możliwości poszczególnych przedstawicieli *constituency* i interesariuszy jako całości.	1-5 roboczodni
10. USŁUGA – DORADZTWO TECHNICZNE.	
OPIS USŁUGI	**Roboczodni**
Usługa, która koncentruje się na rekomendowaniu, opracowywaniu, dostarczaniu i nabywaniu dla interesariuszy infrastruktury, narzędzi i usług związanych z cyberbezpieczeństwem. Wszystkie te systemy i narzędzia odnoszą się do CSIRT/bezpieczeństwa, a nie ogólnie do technologii informacyjnych; systemy te mogą obejmować portale powiadamiania/ostrzegania. Należy zwrócić uwagę, że zespół CSIRT może dostarczyć zainteresowanym stronom pewne narzędzia jako usługę.	5-10 roboczodni
11. USŁUGA – GROMADZENIE I WYKORZYSTANIE NABYTYCH DOŚWIADCZEŃ	
OPIS USŁUGI	**Roboczodni**
Obsługa incydentów jest działaniem reaktywny. W większości przypadków czas na reakcję jest krótki, a początkowa sytuacja niejasna. Pierwotne przyczyny wielu incydentów są ukryte i wymagają usunięcia na późniejszym etapie. Usługa ta ma na celu zapobieganie podobnym incydentom i poprawie reakcji na podobną lub ogólniejszą sytuację.	1-5 roboczodni
12. USŁUGA – ROZWÓJ METODYK ZARZĄDZANIA PODATNOŚCIAMI.	
OPIS USŁUGI	**Roboczodni**
Usługa polegająca na definiowaniu, identyfikacji zdolności i ulepszaniu metodyk świadczenia usług związanych z podatnościami lub koordynacji działań innych podmiotów w tym zakresie.	2-6 roboczodni
13. USŁUGA – ROZWÓJ TECHNOLOGII I PROCESÓW THREAT INTELLIGENCE.	
OPIS USŁUGI	**Roboczodni**
Usługa polegająca na definiowaniu, identyfikacji zdolności i ulepszaniu metodyk niezbędnych do wykonywania usług analizy i rozpowszechniania informacji, związanych z *threat intelligence*.	3-8 roboczodni
14. USŁUGA – ROZWÓJ WŁASNYCH NARZĘDZI CYBERBEZPIECZEŃSTWA.	
OPIS USŁUGI	**Roboczodni**
Usługa polegająca na rozwijaniu, identyfikacji nowych zdolności i współdzieleniu pomysłów dotyczących nowych narzędzi w celu zautomatyzowania procesów CSIRT-u.	2-6 roboczodni
Razem	50-111

Załącznik nr 2 do OSR

Lp.	rodzaj kosztów	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	SUMA
1	koszty realizacji i utrzymania podłączeń do S46 (w tym zakup urządzeń końcowych)	3 358 000	8 212 000	5 941 000	2 823 000	2 605 000	2 678 000	5 592 000	10 392 000	8 367 000	5 513 000	55 481 000
2	koszty rozwoju S46 związanego z nowymi zadaniami	535 000	275 000	286 000	354 000	368 000	677 000	991 000	1 117 000	1 247 000	1 383 000	7 233 000
3	koszty zapewnianie działania systemu	4 618 000	3 638 000	4 451 000	4 280 000	3 702 000	6 551 000	6 417 000	9 532 000	11 445 000	7 468 000	62 102 000
4	koszty pośrednie	1 642 000	2 334 000	2 036 000	1 387 000	1 207 000	1 844 000	2 452 000	4 038 000	3 987 000	2 645 000	23 572 000
	SUMA	**10 153 000**	**14 459 000**	**12 714 000**	**8 844 000**	**7 882 000**	**11 750 000**	**15 452 000**	**25 079 000**	**25 046 000**	**17 009 000**	**148 388 000**

Ad 1	Koszty realizacji i utrzymania podłączeń do S46 (w tym zakup urządzeń końcowych) związane są z koniecznością podłączenia ponad dwukrotnie większej od szacunki z 2018 r. liczby podmiotów krajowego systemu cyberbezpieczeństwa. W skład tych kosztów wchodzą koszty jednorazowe - zakup urządzeń, usług, koszty instalacji oraz koszty ciągłe - koszty łączności i serwisu urządzeń zakończenia sieci dla podłączanych podmiotów celem zmniejszenia bariery finansowej - szczególnie dla podmiotów publicznych (z odnowieniem parku maszynowego - sukcesywnym od 2028 roku)
Ad 2	Koszty rozwoju S46 związane z nowymi zadaniami wynikają ze zmian technologicznych oraz ciągłego dostosowywania S46 do potrzeb rozszerzonego grona jego użytkowników.
Ad 3	Koszty zapewnienie działania systemu zawierają koszty zapewnienia ciągłości działania rozbudowanego systemu S46, koszty odnowienia parku maszynowego (centra) - sukcesywne od 2028 roku, koszty uspójniania modelu cyberbezpieczeństwa w środowisku wielu CSIRT (analizy merytoryczne S46) oraz inne koszty (serwisy, kolokacje, prąd, łączność centrów, materiały, koszty stanowisk pracy, szkoleń, delegacji, transportu, nakłady związane ze zwiększaniem poziomu bezpieczeństwa systemu).
Ad 4	Koszty pośrednie są związane z zapewnieniem administracyjnej obsługi projektu, w tym: koszty dyrekcji (zarządu), obsługi kadrowej czy księgowości. Stanowią ryczałt, odpowiadający 20% sumy wszystkich innych kosztów z wyłączeniem usług.