Projekt z dnia 12 października 2021 r.

U S T A W

z dnia …… 2021 r.

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw [1),2),3)]

Art. 1. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369) wprowadza się następujące zmiany:

1) przed rozdziałem 1 dodaje się oznaczenie i tytuł działu w brzmieniu:

„DZIAŁ I. POSTANOWIENIA OGÓLNE”;

2) w art. 1:

a) w ust. 1:

– po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zasady i tryb certyfikacji produktu ICT, usługi ICT lub procesu ICT w zakresie cyberbezpieczeństwa określonych w rozporządzeniu 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

---

1) Niniejsza ustawa w zakresie swojej regulacji służy stosowaniu 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 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15).

2) Niniejsza ustawa została notyfikowana Komisji Europejskiej w dniu …… pod numerem ……, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), które wdraża postanowienia dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego [ujednolicenie] (Dz. Urz. UE L 241/1 z 17.09.2015, str. 1).

3) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 12 października 1990 r. o Straży Granicznej, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych, ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, ustawę z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego, ustawę z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, ustawę z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym.

cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15), zwanego dalej „rozporządzeniem 2019/881;”,

b) w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4-8 w brzmieniu:

„4) zasady działania Funduszu Cyberbezpieczeństwa;

5) zasady wyznaczania i zadania Operatora strategicznej sieci bezpieczeństwa oraz jego zadania;

6) zasady powoływania i funkcjonowania Spółki Polskie 5G;

7) zasady przyznania zasobów częstotliwości z zakresu 703 – 733 MHz oraz 758 – 788 MHz;

8) zasady działania Funduszu celowego na rzecz strategicznej sieci bezpieczeństwa.”,

c) w ust. 2 pkt 1 i 2 otrzymują brzmienie:

„1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, z wyjątkiem działu II, art. 66a-66c, art. 67a i 67b oraz art. 73 i 74;

2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), z wyjątkiem art. 67a i 67b oraz art. 73 i 74;”;

3) w art. 2:

a) przed pkt 1 dodaje się pkt 1^1-1^3 w brzmieniu:

„1^1) akredytacja - akredytację, o której mowa w art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30), zwanym dalej „rozporządzeniem 765/2008”;

1^2) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i

autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

1[3]) certyfikat – europejski certyfikat cyberbezpieczeństwa lub krajowy certyfikat cyberbezpieczeństwa;”,

b) po pkt 3 dodaje się pkt 3a-3c w brzmieniu:

„3a) CSIRT sektorowy – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora;

3b) CSIRT INT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Wywiadu na rzecz jednostek organizacyjnie podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych oraz Agencji Wywiadu;

3c) dostawca – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, o których mowa w art. 2 pkt 3-6 rozporządzenia 765/2008;”,

c) pkt 4 otrzymuje brzmienie:

„4) cyberbezpieczeństwo – działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami;”,

d) po pkt 4 dodaje się pkt 4a i 4b w brzmieniu:

4a) deklaracja zgodności – oświadczenie dostawcy produktu ICT, usługi ICT lub procesu ICT, że wyrób jest zgodny z europejskim programem certyfikacji cyberbezpieczeństwa, o którym mowa w art. 2 pkt 9 rozporządzenia 2019/881 lub krajowym programem certyfikacji cyberbezpieczeństwa;

4b) ENISA – Agencję Unii Europejskiej do spraw Cyberbezpieczeństwa;”,

e) pkt 5 otrzymuje brzmienie:

„5) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;”,

f) po pkt 9 dodaje się pkt 9a -9f w brzmieniu:

„9a) ISAC – centrum wymiany i analizy informacji na temat podatności cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa;

9b) jednostka oceniająca zgodność – jednostkę oceniającą zgodność, o której mowa w art. 2 pkt 13 rozporządzenia 765/2008;

9c) krajowy certyfikat cyberbezpieczeństwa – certyfikat cyberbezpieczeństwa wydany w ramach krajowego programu certyfikacji cyberbezpieczeństwa;

9d) krajowa deklaracja zgodności – deklaracja zgodności wydana w ramach krajowego programu certyfikacji cyberbezpieczeństwa;

9e) krajowy program certyfikacji cyberbezpieczeństwa – kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych przez Radę Ministrów i mających zastosowanie do certyfikacji lub oceny zgodności objętych zakresem danego programu produktów ICT, usług ICT i procesów ICT;

9f) krajowy poziom uzasadnienia zaufania – potwierdzenie, że dany produkt ICT, dana usługa ICT lub dany proces ICT spełnia wymogi wskazanego poziomu bezpieczeństwa określonego w krajowym programie certyfikacji cyberbezpieczeństwa;”,

g) po pkt 10 dodaje się pkt 10a w brzmieniu:

„10a) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia 765/2008;”,

h) pkt 11 otrzymuje brzmienie:

„11) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez cyberzagrożenia;”,

i) po pkt 11 dodaje się pkt 11a i 11b w brzmieniu:

„11a) proces ICT – zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;

11b) produkt ICT – element lub grupę elementów systemu informacyjnego;”,

j) po pkt 12 dodaje się pkt 12a w brzmieniu:

„12a) SOC – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa;”,

k) po pkt 15 dodaje się pkt 15a w brzmieniu:

15a) usługa ICT – usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych;”,

l) pkt 17 otrzymuje brzmienie:

„17) cyberzagrożenie – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na systemy informacyjne, użytkowników takich systemów oraz innych podmiotów;”;

4) po art. 2 dodaje się oznaczenie i tytuł działu oraz oznaczenie i tytuł rozdziału w brzmieniu:

„DZIAŁ II.

Krajowy system cyberbezpieczeństwa i krajowy system certyfikacji cyberbezpieczeństwa

Rozdział 1

Krajowy system cyberbezpieczeństwa”;

5) po art. 3 dodaje się art. 3a w brzmieniu:

„Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu:

1) identyfikacji źródła i analizy ruchu sieciowego powodującego wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usługi kluczowej, usługi cyfrowej lub realizację zadań publicznych,
2) czasowego ograniczenia ruchu sieciowego z adresów IP lub adresów URL, zidentyfikowanego jako przyczyna incydentu, wchodzącego do infrastruktury tego podmiotu.”;

6) użyte w art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2, w art. 11 w ust. 3 we wprowadzeniu do wyliczenia, w art. 12 w ust. 3 i 4, w art. 13 w ust. 3, w art. 14 ust. 3, w art. 15 w ust. 2 w pkt 3, w art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5 dwukrotnie, w art. 44 w ust. 1 we wprowadzeniu do wyliczenia, w ust. 2, w ust. 3 w zdaniu pierwszym i drugim oraz w ust. 4, w art. 48 w pkt 1, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 64, w art. 65 w ust. 1 w pkt 2 i 4, w art. 66 w ust. 7 oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa”, zastępuje się użytymi w odpowiedniej liczbie i przypadku wyrazami „CSIRT sektorowy”;

7) w art. 4:

a) po pkt 6 dodaje się pkt 6a i 6b w brzmieniu:

„6a) CSIRT INT;

6b) ISAC, o którym mowa w art. 25a;”,

b) w pkt 7 wyrazy „w art. 9 pkt 1-6, 8, 9, 11 i 12” zastępuje się wyrazami „w art. 9 pkt 1-6, 8-10”,

c) po pkt 7 dodaje się pkt 7a w brzmieniu:

„7a) Urząd Komisji Nadzoru Finansowego;”,

d) pkt 8 otrzymuje brzmienie:

„8) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3-7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2020 r. poz. 478, 619 i 1630);”,

e) po pkt 14 dodaje się pkt 14a i14b w brzmieniu:

„14a)Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. - Prawo wodne (Dz. U. z 2021 r. poz. 624, 784, 1564 i 1641);

14b) Polski Fundusz Rozwoju oraz inne instytucje rozwoju, o których mowa w ustawie z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2021 r. poz. 1010);”,

f) pkt 16 otrzymuje brzmienie:

„16) podmioty niebędące operatorem usługi kluczowej, świadczące usługi SOC na rzecz operatora usługi kluczowej;”;

8) w art. 7:

a) w ust. 4 wyrazy „nie później niż w terminie 6 miesięcy” zastępuje się wyrazami „niezwłocznie, nie później niż w terminie 1 miesiąca”;

b) ust. 5 otrzymuje brzmienie:

„5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.”;

9) użyte w art. 8 w pkt 3, w pkt 5 w lit. d, w art. 9 w ust. 1 w pkt 2, w art. 13 w ust. 1 w pkt 2, w art. 22 w ust. 1 w pkt 4, w art. 26 w ust. 1, w ust. 3 w pkt 1, 2, 4 i 10, w pkt 14 w lit. b i c i w ust. 6 w pkt 2, w art. 33 w ust. 4a, w art. 35 w ust. 4 i 5, w art. 37 w ust. 1, w art. 39 w ust. 1, 3 i 4, w art. 46 w ust. 1 w pkt 5, w art. 51 w pkt 2, 7 i 8, w art. 52 w pkt 2 i 4, w art. 53 w ust. 1 w pkt 2 w lit. a, w art. 62 w ust. 2 w pkt 3, w art. 65 w ust. 1 w pkt 1 i 2, w art. 73 w ust. 5 w pkt 1, w art. 83, w różnej liczbie i różnym przypadku, wyrazy „zagrożenie cyberbezpieczeństwa” zastępuje się użytym w odpowiedniej liczbie i przypadku wyrazem „cyberzagrożenie”;

10) w art. 8 w pkt 5 lit. b otrzymuje brzmienie:

„b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz poziomu krytyczności poszczególnych aktualizacji,”;

11) w art. 9:

a) w ust. 1 w pkt 1 wyrazy „osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”,

b) ust. 2 otrzymuje brzmienie:

„2. Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa dane osób, o których mowa w ust. 1 pkt 1, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych - w terminie 14 dni od dnia ich zmiany. Organ właściwy do spraw cyberbezpieczeństwa przekazuje te dane do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego.”;

12) w art. 10:

a) w ust. 1, ust. 2 we wprowadzeniu do wyliczenia oraz w ust. 3 i 4 wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”,

b) w ust. 2 pkt 2 otrzymuje brzmienie:

„2) ochronę dokumentów przed przypadkowym uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;”,

c) w ust. 5 wyraz „cyberbezpieczeństwa” zastępuje się wyrazami „bezpieczeństwa systemów informacyjnych”;

13) w art. 11:

a) w ust. 1 w pkt 4 wyrazy „ CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”.;

b) w ust. 2 po wyrazach „przekazywane jest w postaci elektronicznej” dodaje się wyrazy „za pomocą systemu, o którym mowa w art. 46 ust. 1”;

c) w ust. 3:

– pkt 1 i 2 otrzymują brzmienie:

„1) współdziała z właściwym CSIRT sektorowym na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, koordynowanej przez CSIRT GOV, CSIRT MON lub CSIRT NASK, przekazując niezbędne dane, w tym dane osobowe;

2) zapewnia właściwemu CSIRT sektorowemu dostęp do informacji o rejestrowanych incydentach.”;

– uchyla się pkt 3;

13) w art. 13:

a) w ust. 1 wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”;

b) uchyla się ust. 3

c) dodaje się ust. 5 w brzmieniu:

„5. CSIRT sektorowy niezwłocznie, nie później niż w ciągu 8 godzin, przekazuje do właściwego CSIRT GOV, CSIRT MON albo CSIRT NASK informacje o których mowa w ust. 1”;

14) art. 14 otrzymuje brzmienie:

„Art. 14. 1. Zadania operatora usługi kluczowej, o których mowa w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13, w zakresie bezpieczeństwa systemów informacyjnych realizowane są w ramach SOC.

2. Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury lub zawiera umowę o prowadzenie SOC, zwaną dalej „umową o prowadzenie SOC”, albo realizuje zadania poprzez SOC utworzony na jego rzecz przez organ tworzący lub nadzorujący.

3. SOC powołany przez operatora usługi kluczowej może realizować zadania, o których mowa w ust. 1, także na rzecz innych podmiotów.

4. SOC, na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, z uwzględnieniem określenia zasad dostępu do pomieszczeń oraz systemów, a także eksploatacji i architektury systemów, w celu:

1) monitorowania i wykrywania incydentów;

2) reagowania na incydenty;

3) zapobiegania incydentom;

4) zarządzania jakością zabezpieczeń systemów, informacji i aktywów;

5) aktualizowania analizy ryzyka w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na działania, o których mowa w pkt 1.

5. Operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o sposobie realizacji obowiązku, o którym mowa w ust. 2, polegającego na powołaniu SOC wewnątrz swojej struktury lub zawarciu umowy o prowadzeniu SOC, albo realizowaniu zadania poprzez SOC utworzony na jego rzecz przez organ tworzący lub nadzorujący , lub o zmianie sposobu realizacji tego obowiązku.

6. W przypadku zawarcia umowy o prowadzenie SOC operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o:

1) zawarciu takiej umowy,
2) danych kontaktowych, o których mowa w ust. 8 pkt 4, podmiotu, z którym zawarta została umowa,
3) zakresie świadczonej usługi,
4) terminie obowiązywania umowy,
5) rozwiązaniu umowy

– w terminie 14 dni od dnia zawarcia lub rozwiązania umowy.

7. W przypadku, gdy jest to niezbędne dla zapewnienia bezpieczeństwa systemów informacyjnych, podmiot prowadzący SOC zapewnia bezpieczny i zdalny dostęp do swoich systemów obsługiwanemu operatorowi usługi kluczowej przez co najmniej:

1) ustalenie zasad dostępu do systemu;
2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację;
3) minimalizację zakresu danych przechowywanych poza bezpiecznym środowiskiem.

8. Przy zawieraniu umowy o prowadzenie SOC zawiera się zastrzeżenie, że świadczenie tych usług podlega prawu polskiemu.

9. Podmiot niebędący operatorem usługi kluczowej, świadczący usługi SOC na rzecz operatora usługi kluczowej, udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:

1) nazwa SOC;
2) zakres obszaru działania, w tym:
   a) oferowany rodzaj wsparcia,
   b) zasady współpracy i wymiany informacji,
   c) politykę komunikacji i uwierzytelniania informacji;

3) oferowane usługi oraz politykę obsługi incydentów i koordynacji incydentów;
4) dane kontaktowe, w tym:
   a) adres ze wskazaniem strefy czasowej,
   b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC,
   c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z SOC,
   d) sposoby kontaktu z SOC, w tym sposób zgłaszania incydentów.”;

15) po art. 14 dodaje się art. 14a w brzmieniu:

„14a. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz SOC.

2. Wykaz SOC zawiera:

1) nazwę (firmę) podmiotu prowadzącego SOC;
2) nazwę (firmę) podmiotów, na rzecz których SOC jest prowadzony;
3) siedzibę i adres SOC;
4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) datę wpisania do wykazu SOC;
7) datę wykreślenia z wykazu SOC.

3. Wpisanie do wykazu SOC i wykreślenie z tego wykazu następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa złożony niezwłocznie, nie później niż w terminie 14 dni, po uzyskaniu od operatora usługi kluczowej informacji, o której mowa w art. 14 ust. 4 lub informacji, o której mowa w art. 14 ust. 5. Wniosek zawiera dane, o których mowa w ust. 2 pkt 1-5.

4. Zmiana danych w wykazie SOC następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa, złożony niezwłocznie, nie później niż w terminie miesiąca od zmiany tych danych.

5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

6. Wpisanie do wykazu SOC i wykreślenie z tego wykazu oraz zmiana danych w wykazie SOC są czynnościami materialno-technicznymi.

7. Minister właściwy do spraw informatyzacji może, z urzędu, wpisać do wykazu, o którym mowa w ust. 1, również SOC niepowołany wewnątrz struktury operatora usługi kluczowej ani niebędący stroną umowy o SOC, jeżeli co najmniej:

1) świadczy usługi z zakresu cyberbezpieczeństwa, w szczególności związane z:
   a) monitorowaniem, wykrywaniem, reagowaniem i zapobieganiem incydentów,
   b) zarządzaniem jakością zabezpieczeń systemów, informacji i powierzonych aktywów,
   c) aktualizowaniem ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent;
2) przedstawi dokument potwierdzający zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742),
3) zawrze z ministrem właściwym do spraw informatyzacji porozumienie w sprawie korzystania z systemu, o którym mowa w art. 46 ust. 1.

8. Minister właściwy do spraw informatyzacji wykreśla z wykazu wpisany z urzędu SOC, który przestał spełniać warunki, o których mowa w ust. 7.

9. Dane z wykazu SOC minister właściwy do spraw informatyzacji udostępnia CSIRT GOV, CSIRT MON, CSIRT NASK i CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, a także operatorowi usługi kluczowej w zakresie go dotyczącym.

10. Minister właściwy do spraw informatyzacji udostępnia dane z wykazu SOC, na wniosek, następującym podmiotom:

1) organowi właściwemu do spraw cyberbezpieczeństwa,
2) Policji,
3) Żandarmerii Wojskowej,
4) Straży Granicznej,
5) Centralnemu Biuru Antykorupcyjnemu,
6) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,
7) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego,
8) sądom,
9) prokuraturze,
10) organom Krajowej Administracji Skarbowej,
11) dyrektorowi Rządowego Centrum Bezpieczeństwa,

12) Służbie Ochrony Państwa

– w zakresie niezbędnym do realizacji ich ustawowych zadań.”;

16) użyty w art. 17 w ust. 2, art. 69 w ust. 1, w ust. 2 w pkt 1, 6 i 7, w różnej liczbie i przypadku, wyraz „cyberbezpieczeństwo” zastępuje się użytymi w odpowiedniej liczbie i przypadku wyrazami „bezpieczeństwo systemów informacyjnych”;

17) w art. 17 w ust. 2 pkt 1 skreśla się wyrazy „systemów informacyjnych i”;

18) w art. 21:

a) w ust. 1 wyrazy „osoby odpowiedzialnej” zastępuje się wyrazami „dwóch osób odpowiedzialnych”;

b) w ust. 2 i 3 wyrazy „jedną osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”;

19) w art. 22:

a) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Agencja Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zgłaszają incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT INT.”;

b) w ust. 2 po wyrazach „w ust. 1 pkt 2” dodaje się wyrazy „ ust. 1a”;

c) dodaje się ust. 3 - 7 w brzmieniu:

„3. Niezależnie od zadań, określonych w ust. 1, Agencja Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, przekazuje jednocześnie CSIRT INT w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, zgłoszenie, o którym mowa w ust. 1 pkt 4;

4. Jednostki, o których mowa w ust. 3, współdziałają z CSIRT INT podczas obsługi incydentu w podmiocie publicznym, przekazując niezbędne dane, w tym dane osobowe.

5. Jednostki, o których mowa w ust. 3, zapewniają CSIRT INT dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.

6. Agencja Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, przekazują do CSIRT INT dane osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

7. CSIRT INT niezwłocznie przekazuje informacje, o których mowa w ust. 6, do CSIRT GOV.”;

20) w art. 23 w ust. 3 i 4 oraz w art. 24 w zdaniu pierwszym wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT”;

21) po art. 25 dodaje się rozdział 5a w brzmieniu:

„Rozdział 5a

Zadania i obowiązki ISAC w ramach krajowego systemu cyberbezpieczeństwa

Art. 25a. 1. W ramach krajowego systemu cyberbezpieczeństwa może funkcjonować ISAC, do którego zadań należy w szczególności wymiana informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów.

2. Minister właściwy do spraw informatyzacji prowadzi wykaz ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa, zwany dalej „wykazem ISAC”.

3. Wykaz ISAC zawiera:

1) nazwę (firmę) ISAC;

2) imię i nazwisko osoby reprezentującej ISAC wraz z numerem telefonu oraz adres poczty elektronicznej;
3) siedzibę i adres ISAC, jeżeli posiada;
4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) datę wpisania do wykazu ISAC;
7) datę wykreślenia z wykazu ISAC;
8) informację o korzystaniu przez ISAC z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

4. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa. Wniosek zawiera dane, o których mowa w ust. 3 pkt 1-5 oraz opinię wnioskodawcy o ISAC.

5. Zmiana danych w wykazie ISAC następuje na wniosek podmiotu prowadzącego ISAC, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych, lub z urzędu.

6. Wnioski, o których mowa w ust. 4 i 5, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

7. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych w wykazie ISAC są czynnościami materialno-technicznymi.

8. Wykaz ISAC jest publikowany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.

9. ISAC wpisany do wykazu ISAC współpracuje z CSIRT GOV, CSIRT MON lub CSIRT NASK, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa, w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów.

10. ISAC wpisane do wykazu ISAC przedkładają ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.

11. Minister właściwy do spraw informatyzacji, na wniosek organu właściwego albo urzędu, może przeprowadzić kontrolę:

1) zgodności z prawem działania ISAC wpisanego do wykazu ISAC;

2) przestrzegania przez ISAC wpisanego do wykazu ISAC, zasad współpracy w ramach krajowego systemu bezpieczeństwa.

12. Do kontroli, o której mowa w ust. 11, przepis art. 54 ust. 2 stosuje się odpowiednio.

13. W razie stwierdzenia, że działalność ISAC wpisanego do wykazu ISAC jest niezgodna z prawem lub narusza zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa, minister właściwy do spraw informatyzacji, w zależności od rodzaju i stopnia stwierdzonych nieprawidłowości, może:

1) wystąpić do ISAC o usunięcie stwierdzonych nieprawidłowości w określonym terminie lub
2) wykreślić ISAC z wykazu ISAC.”;

22) w art. 26:

a) ust. 2 otrzymuje brzmienie:

„2. CSIRT GOV, CSIRT MON i CSIRT NASK w uzasadnionych przypadkach na wniosek podmiotów krajowego systemu cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów.”,

b) po ust. 2 dodaje się ust. 2a i 2b w brzmieniu:

„2a. Pełnomocnik może zlecić CSIRT NASK zapewnienie wsparcia w obsłudze incydentów, o których mowa w ust. 2.

2b. Pełnomocnik, za zgodą, Szefa Agencji Bezpieczeństwa Wewnętrznego albo Ministra Obrony Narodowej, może zlecić CSIRT GOV albo CSIRT MON zapewnienie wsparcia w obsłudze incydentów, o których mowa w ust. 2. Zgoda może być wyrażona w szczególności z wykorzystaniem środków porozumiewania się na odległość.”,

c) w ust. 3:

– pkt 5 otrzymuje brzmienie:

„5) reagowanie na incydenty oraz koordynacja reagowania na zgłoszone incydenty;”,

– w pkt 10 po wyrazie „oraz” dodaje się wyrazy „z CSIRT INT”;

– w pkt 12 wyrazy „30 maja” zastępuje się wyrazami „31 stycznia”,

– pkt 16 otrzymuje brzmienie:

„16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)”,

– w pkt 16 kropkę zastępuje się średnikiem i dodaje się pkt 17-22 w brzmieniu:

„17) gromadzenie oraz przetwarzanie informacji dotyczących cyberzagrożeń, podatności i incydentów;

18) przygotowywanie na zlecenie Pełnomocnika lub przewodniczącego Kolegium analiz w zakresie cyberzagrożeń, podatności i incydentów;

19) przygotowywanie na zlecenie Pełnomocnika analiz skutków incydentów oraz przebiegu obsługi incydentów;

20) przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa;

21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności przez:

a) wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi do spraw cyberbezpieczeństwa i podmiotem krajowego systemu cyberbezpieczeństwa, u którego wykonywany jest test,

b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.”;

22) udział w przedsięwzięciach mających na celu rozwój kompetencji CSIRT GOV, CSIRT MON lub CSIRT NASK, w szczególności w ćwiczeniach oraz szkoleniach specjalistycznych.”,

d) po ust. 3 dodaje się ust. 3a w brzmieniu:

„3a. Do testów bezpieczeństwa, o których mowa w ust. 3 pkt 21 lit. a stosuje się odpowiednio przepisy art. 32a ust. 4 –6 i 9 – 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27 i 2320).”,

e) w ust. 4 wyrazy „sektorowymi zespołami cyberbezpieczeństwa” „zastępuje się wyrazami „CSIRT sektorowy i CSIRT INT”;

f) w ust. 6 w pkt 1:

– lit. a otrzymuje brzmienie:

„a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2-6 i 10 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,”,

– lit. c otrzymuje brzmienie:

„c) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3-7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce,”,

g) w ust. 7 po pkt 4 dodaje się pkt 4a- 4c w brzmieniu:

„4a) Państwowe Gospodarstwo Wodne Wody Polskie;

4b) Polski Fundusz Rozwoju i inne instytucje rozwoju;

4c) Urząd Komisji Nadzoru Finansowego;”,

h) ust. 9 otrzymuje brzmienie:

„9. Działalność bieżąca CSIRT NASK jest finansowana w formie dotacji podmiotowej ze środków, których dysponentem jest minister właściwy do spraw informatyzacji.”,

i) po ust. 9 dodaje się ust. 9a w brzmieniu:

„9a. W zakresie nieobjętym finansowaniem, o którym mowa w ust. 9, działalność CSIRT NASK może być finansowana z innych źródeł, w szczególności:

1) ze środków pozyskanych przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy w związku z uczestnictwem w krajowych, regionalnych lub unijnych konkursach lub programach operacyjnych,

2) z przychodów z działalności Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.”,

j) dodaje się ust. 12 w brzmieniu:

„12. Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego lub minister właściwy do spraw informatyzacji informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w ust. 10. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.”;

23) użyte w art. 26 w ust. 3 w pkt 16 oraz w art. 49 w ust. 3 w pkt 2 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”;

24) w art. 31 w ust. 2 dodaje się zdanie drugie w brzmieniu: „Komunikat podlega również publikacji w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.”;

25) art. 32 ust. 4 otrzymuje brzmienie:

„4. CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT lub CSIRT sektorowy na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotów krajowego systemu cyberbezpieczeństwa mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.”;

26) w art. 33:

a) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Badanie, o którym mowa w ust. 1, przeprowadza się także na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium, skierowany do organu prowadzącego lub nadzorującego właściwy zespół CSIRT, celem weryfikacji informacji będących w dyspozycji Kolegium, dotyczących możliwych podatności.”,

b) w ust. 2 wyrazy „pozostałe CSIRT” zastępuje się wyrazami „pozostałe CSIRT MON, CSIRT NASK i CSIRT GOV”,

c) po ust. 4b dodaje się ust. 4c w brzmieniu:

„4c. Rekomendacje, o których mowa w ust. 4, a także informację o ich zmianie lub odwołaniu, Pełnomocnik publikuje w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.”;

27) w art. 34 ust. 1 otrzymuje brzmienie:

„1. CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy oraz SOC współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”;

28) w art. 35 ust. 5 otrzymuje brzmienie:

"5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą przekazywać Pełnomocnikowi do publikacji na stronie podmiotowej Pełnomocnika w Biuletynie Informacji Publicznej informacje o podatnościach, incydentach krytycznych oraz o cyberzagrożeniach:

1) jeżeli przekazywanie tych informacji przyczyni się do zwiększenia bezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów,

2) wyłącznie w zakresie niezbędnym do realizacji tych celów, oraz

3) jeżeli publikacja informacji nie będzie naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych.";

29) w art. 36:

a) ust. 2 otrzymuje brzmienie:

„2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, Pełnomocnika, ministra właściwego do spraw informatyzacji oraz Rządowego Centrum Bezpieczeństwa.”,

b) w ust. 6 zdanie pierwsze otrzymuje brzmienie:

„Dyrektor Rządowego Centrum Bezpieczeństwa na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 1, zawiadamia niezwłocznie członków Zespołu i Pełnomocnika o terminie i miejscu posiedzenia Zespołu.”;

30) po art. 36 dodaje się art. 36a w brzmieniu:

„Art. 36a. W wypadku wystąpienia incydentu krytycznego Prezes Rady Ministrów może, na podstawie opinii Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia CSIRT koordynującemu obsługę tego incydentu przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.”;

31) po art. 36a dodaje się rozdział 6a w brzmieniu:

„Rozdział 6a

Zadania CSIRT INT

Art. 36b. 1. Do zadań CSIRT INT należy zapewnianie wsparcia w obsłudze incydentów zgłaszanych przez:

1) jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

2) Agencję Wywiadu.

2. W zakresie określonym w ust. 1 CSIRT INT współpracuje z CSIRT GOV.

3. Do zadań CSIRT INT w ramach wspierania podmiotów określonych w ust. 1 należy:

1) przyjmowanie zgłoszeń o incydentach w podmiotach publicznych;
2) reagowanie na incydenty w podmiotach publicznych;
3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo w podmiotach publicznych;
4) współpraca z podmiotami publicznymi w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestnictwo w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty w podmiotach publicznych oraz wymiany informacji o cyberzagrożeniach;
6) zapewnianie dynamicznej analizy ryzyka i incydentów oraz wspomaganie podnoszenia świadomości o cyberzagrożeniach;
7) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych, podmiotów o których mowa w ust. 1 , w szczególności przez:
   a) wykonywanie testów bezpieczeństwa w porozumieniu z podmiotami, o których mowa w ust. 1,
   b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.

4. Do testów bezpieczeństwa, o których mowa w ust. 3 pkt 7 lit. a stosuje się odpowiednio przepisy art. 32a ust. 4–6 i 9–11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

Art. 36c. CSIRT INT niezwłocznie, nie później niż w ciągu 8 godzin, przekazuje zgłoszenie, o którym mowa w art. 22 ust. 1a , do CSIRT GOV.”;

32) w art. 37:

a) ust. 1 otrzymuje brzmienie:

„1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176 oraz z 2021 r. poz. 1598

i 1641) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641).”,

b) ust. 2 i 3 otrzymują brzmienie:

„2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent operatorem usługi kluczowej, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.

3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, informacje o incydentach istotnych lub wystąpić do organu właściwego do spraw cyberbezpieczeństwa dla dostawcy usług cyfrowych, aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu, albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym.”;

33) w art. 39:

a) w ust. 1 po wyrazach „CSIRT GOV” dodaje się wyrazy „„CSIRT INT”;

b) użyte w ust. 1 i 2, w ust. 3 we wprowadzeniu do wyliczenia oraz ust. 5-9, w różnej liczbie wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie wyrazami „CSIRT sektorowy”,

c) w ust. 3:

– we wprowadzeniu do wyliczenia po wyrazach „CSIRT GOV” dodaje się wyrazy „„CSIRT INT”,

– pkt 2 otrzymuje brzmienie:

„2) dotyczące telekomunikacyjnych urządzeń końcowych;”,

d) w ust. 7 po wyrazach „CSIRT GOV” dodaje się wyrazy „„CSIRT INT”;

34) w art. 40:

a) w ust. 1- 3 wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”,

b) w ust. 1- 3 po wyrazach „CSIRT GOV” dodaje się wyrazy „„CSIRT INT”;

35) w art. 42:

a) w ust. 1:

– pkt 4 otrzymuje brzmienie:

„4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych bezzwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych;”,

– w pkt 5 i 7 po wyrazach „CSIRT MON” dodaje się wyrazy „„CSIRT INT”,

b) uchyla się ust. 3–6,

c) w ust. 8 wyrazy „Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazami „ENISA”;

36) w art. 44:

a) ust. 1 otrzymuje brzmienie:

„1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 do ustawy, do którego zadań należy:

1) przyjmowanie zgłoszeń o incydentach;

2) reagowanie na incydenty;

3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych;

4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;

5) współpraca z CSIRT GOV, CSIRT MON i CSIRT NASK w koordynowanym przez nie reagowania na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów;

6) współpraca z innymi CSIRT sektorowymi oraz CSIRT INT w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.”,

b) po ust. 1 dodaje się ust. 1a-1c w brzmieniu:

1a. CSIRT sektorowy niezwłocznie, nie później niż 8 godzin od jego otrzymania, przekazuje zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4 do właściwego CSIRT GOV, CSIRT MON albo CSIRT NASK.

1b. CSIRT sektorowy może, w szczególności:

1) zapewniać we współpracy z CSIRT GOV, CSIRT MON i CSIRT NASK dynamiczną analizę ryzyka i analizę incydentów oraz wspomagać w

podnoszeniu świadomości cyberzagrożeń wśród operatorów usług kluczowych danego sektora lub podsektora;

2) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które ich dotyczą;

3) wspierać, w uzgodnieniu z operatorem usługi kluczowej, wykonywanie przez niego obowiązków określonych w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13;

4) zwracać się do CSIRT GOV, CSIRT MON, CSIRT NASK o wystąpienie z wnioskiem o którym mowa w art 42 ust. 1 pkt 7;

5) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych operatorów usług kluczowych w danym sektorze, w szczególności przez:

a) wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi i operatorami usług kluczowych,

b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.

1c. Do testów bezpieczeństwa, o których mowa w ust. 1a pkt 5 lit. a stosuje się odpowiednio przepisy art. 32a ust. 4–6 i 9–11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

1d. Realizacja zadań, o których mowa w ust. 1b pkt 5, odbywa się za zgodą CSIRT GOV, CSIRT MON i CSIRT NASK.”,

c) uchyla się ust. 2,

d) dodaje się ust. 5-13 w brzmieniu:

„5. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadań CSIRT sektorowego jednostkom jemu podległym albo przez niego nadzorowanym.

6. Organ właściwy do spraw cyberbezpieczeństwa może, w drodze porozumienia, wyznaczyć spośród jednostek jemu podległych albo przez niego nadzorowanych jednostkę, która będzie wykonywała zadania CSIRT sektorowego dla kilku sektorów. Organy właściwe do spraw cyberbezpieczeństwa określają w porozumieniu zasady sprawowania nadzoru nad CSIRT sektorowym.

7. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć CSIRT GOV, CSIRT MON albo CSIRT NASK realizację zadań CSIRT sektorowego.

8. Powierzenie, o którym mowa w ust. 7 następuje na podstawie porozumienia organu właściwego do spraw cyberbezpieczeństwa:

1) w przypadku powierzenia zadań CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji – z Dyrektorem Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytutem Badawczym;
2) w przypadku powierzenia zadań CSIRT GOV – z Szefem Agencji Bezpieczeństwa Wewnętrznego;
3) w przypadku powierzenia zadań CSIRT MON – z Ministrem Obrony Narodowej.

9. W porozumieniu, o którym mowa w ust. 8, określa się zasady sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań.

10. Komunikat o zawarciu porozumienia, o którym mowa w ust. 6 i 8, ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa. W komunikacie wskazuje się informacje o:

1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami;
2) terminie, od którego porozumienie będzie obowiązywało.

11. Organ właściwy do spraw cyberbezpieczeństwa, informuje Pełnomocnika, o zawarciu porozumienia, o którym mowa w ust. 6 i 8. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej .

12. W budżecie państwa tworzy się rezerwę celową na finansowanie utworzenia oraz funkcjonowania CSIRT sektorowych. Dysponentem rezerwy celowej jest minister właściwy do spraw informatyzacji.

13. Organ właściwy do spraw cyberbezpieczeństwa raz w roku, do dnia 31 grudnia, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT sektorowego. W sprawozdaniu za rok, w którym utworzony został CSIRT sektorowy, zawiera się informacje dotyczące jego utworzenia oraz funkcjonowania.”;

37) w art. 45 w ust. 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 i 8 w brzmieniu:

„7) wydawanie poleceń zabezpieczających;

8) prowadzenie postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka.”;

38) w art. 46:

a) ust. 2 otrzymuje brzmienie:

„2. Pełnomocnik, CSIRT GOV, CSIRT MON, CSIRT NASK oraz operatorzy usług kluczowych korzystają z systemu teleinformatycznego, o którym mowa w ust. 1.”,

b) po ust. 2 dodaje się ust. 2a – 2c w brzmieniu:

„2a. CSIRT sektorowe, CSIRT INT, Prezes Urzędu Komunikacji Elektronicznej korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie swojej właściwości.

2b. Szczegółowe zasady korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, określa porozumienie zawarte pomiędzy ministrem właściwym do spraw informatyzacji, a podmiotem, o którym mowa w ust. 2 i 2a.

2c. Podmioty krajowego systemu cyberbezpieczeństwa, inne niż wskazane w ust. 2 i 2a, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.”;

c) uchyla się ust. 3;

39) w art. 48 w pkt 1 po wyrazach „CSIRT GOV” dodaje się wyrazy „CSIRT INT”;

40) w art. 51:

a) pkt 5 otrzymuje brzmienie:

„5) kierowanie, za pośrednictwem CSIRT MON, działaniami związanymi z obsługą incydentów w czasie stanu wojennego;”,

b) pkt 7 otrzymuje brzmienie:

„7) ocenę cyberzagrożeń oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;”;

41) tytuł rozdziału 11 otrzymuje brzmienie:

„Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i SOC”;

42) w art. 53 w ust. 1 pkt 1 otrzymuje brzmienie:

„1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi SOC, o których mowa w art. 14a ust. 1, wymogów, o których mowa w art. 14 ust. 3-7;”;

43) po rozdziale 11 dodaje się rozdziały 11a w brzmieniu:

„Rozdział 11a

Krajowy system certyfikacji cyberbezpieczeństwa

Art. 59a. 1. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje:

1) ministra właściwego do spraw informatyzacji;
2) Polskie Centrum Akredytacji;
3) jednostki oceniające zgodność prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa;
4) dostawców produktów ICT, usług ICT lub procesów ICT, którzy poddają swoje wyroby procesowi oceny zgodności zgodnie z ustawą.

2. Nadzór nad funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa sprawuje minister właściwy do spraw informatyzacji.

Art. 59b. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:

1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z certyfikacją cyberbezpieczeństwa;
2) monitorowanie stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, rozporządzenia 2019/881 oraz postanowień krajowych i europejskich programów certyfikacyjnych;
3) przeprowadzanie kontroli w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 59a ust. 1 pkt 3 i 4;
4) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881;

5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy;
6) zatwierdzanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki”;
7) zatwierdzanie krajowych certyfikatów cyberbezpieczeństwa o krajowym poziomie uzasadnienia zaufania „wysoki”;
8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa;
9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymogami rozporządzenia 2019/881 lub z wymogami określonych europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym programie certyfikacji cyberbezpieczeństwa;
10) rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez nie działań związanych z certyfikacją cyberbezpieczeństwa;
11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i;
12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG”, corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b-d oraz ust. 8 rozporządzenia 2019/881;
13) uczestnictwo w pracach ECCG;
14) prowadzenie postępowań w zakresie cofnięcia certyfikatu;
15) nadzorowanie i egzekwowanie zawartych w europejskim programie certyfikacji cyberbezpieczeństwa i krajowych programach certyfikacji cyberbezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku;

Art. 59c. Polskie Centrum Akredytacji sprawuje nadzór nad jednostkami oceniającymi zgodność, w zakresie spełniania przez nie warunków, o których mowa w:

1) art. 24 ust. 3 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2021 r. poz. 514 i 925);
2) załączniku nr 1 do rozporządzenia 2019/881;

3) poszczególnych europejskich programach certyfikacji cyberbezpieczeństwa i krajowych programach certyfikacji cyberbezpieczeństwa.

Art. 59d. 1. Minister właściwy do spraw informatyzacji przygotowuje projekt krajowego programu certyfikacji cyberbezpieczeństwa lub zleca jego przygotowanie jednostkom podległym lub przez niego nadzorowanym..

2. Rada Ministrów może określić, w drodze rozporządzenia, krajowy program certyfikacji cyberbezpieczeństwa dla danego produktu ICT, usługi ICT lub procesu ICT, uwzględniając konieczność opracowania wymagań dla produktów ICT, usług ICT lub procesów ICT zgodnie z aktualną wiedzą naukowo-techniczną oraz mając na celu zwiększenie cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

Art. 59e. 1. Podmiot ubiegający się o certyfikat lub posiadający certyfikat wydany na podstawie krajowego programu certyfikacji cyberbezpieczeństwa jest obowiązany wykonywać obowiązki określone w tym programie.

2. Obowiązki, o których mowa w ust. 1, mogą obejmować w szczególności:

1) udostępnianie informacji niezbędnych do przeprowadzenia certyfikacji;
2) przeprowadzanie okresowych badań produktów ICT, usług ICT, procesów ICT;
3) przeprowadzanie aktualizacji oprogramowania;
4) przeprowadzanie okresowych testów cyberbezpieczeństwa;
5) określony sposób przechowywania dokumentacji związanej z produktem ICT, usługą ICT lub procesem ICT;
6) określony sposób postępowania z wykrytymi podatnościami, w szczególności ich eliminację.

Art. 59f. 1. Tryb postępowań certyfikacyjnych produktów ICT, usług ICT lub procesów ICT może zostać określony w krajowym programie certyfikacji cyberbezpieczeństwa opracowanych odpowiednio dla produktów ICT, usług ICT albo procesów ICT.

2. Krajowy program certyfikacji cyberbezpieczeństwa zawiera:

1) przedmiot i zakres programu certyfikacji, w tym rodzaj lub kategorie objętych danym programem produktów ICT, usług ICT lub procesów ICT, określenie przedmiotu i zakresu programu certyfikacji;
2) opis celu programu oraz wpływu wybranych norm, metod oceny i krajowych poziomów uzasadnienia zaufania na realizację potrzeb przewidywanych użytkowników programu;

3) wskazanie, czy w ramach programu dozwolone jest wydanie deklaracji zgodności;
4) szczegółowe lub dodatkowe wymogi, którym podlegają jednostki oceniające zgodność w celu zagwarantowania ich kwalifikacji technicznych odnośnie do oceny wymogów cyberbezpieczeństwa;
5) szczegółowe kryteria oceny i metody, w tym rodzaje oceny, stosowane w celu wykazania, że zostały osiągnięte cele w zakresie cyberbezpieczeństwa;
6) zakres informacji niezbędnych do uzyskania certyfikatu, które wnioskodawca ma dostarczyć lub udostępnić w inny sposób jednostkom oceniającym zgodność;
7) w przypadku gdy program przewiduje stosowanie znaków lub etykiet poświadczających zgodność z programem – określenie warunków, na jakich takie znaki lub etykiety mogą być stosowane;
8) sposób monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymogami krajowych certyfikatów cyberbezpieczeństwa lub deklaracjami zgodności, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami cyberbezpieczeństwa;
9) szczegółowe warunki wydawania, utrzymywania, przedłużania i odnawiania ważności krajowych certyfikatów cyberbezpieczeństwa,;
10) skutki dla produktów ICT, usług ICT lub procesów ICT, które uzyskały krajowy certyfikat cyberbezpieczeństwa lub w przypadku których wydana została deklaracja zgodności, które nie spełniają wymogów programu;
11) szczegółowy sposób zgłaszania uprzednio niewykrytych, a wpływających na cyberbezpieczeństwo podatności produktów ICT, usług ICT lub procesów ICT, do jego dostawcy oraz sposobu postępowania z nimi;
12) instrukcje dotyczące przechowywania dokumentów przez jednostki oceniające zgodność;
13) treść i wzór graficzny krajowych certyfikatów cyberbezpieczeństwa i krajowych deklaracji zgodności okres dostępności krajowych deklaracji zgodności, dokumentacji technicznej oraz innych istotnych informacji;
14) okres ważności krajowych certyfikatów cyberbezpieczeństwa;
15) sposób dostarczania i aktualizowania dodatkowych informacji na temat cyberbezpieczeństwa przez dostawców sprzętu lub oprogramowania zgodnie z art. 59u.

3. Dostawca certyfikowanych produktów ICT, usług ICT lub procesów ICT lub ubiegający się o uzyskanie certyfikatu jest obowiązany dostarczyć lub udostępnić w inny sposób jednostkom oceniającym zgodność informacje, o których mowa w ust. 2 pkt 6 i 15.

Art. 59g. 1. Krajowy program certyfikacji cyberbezpieczeństwa wskazuje jeden lub więcej krajowych poziomów uzasadnienia zaufania produktów ICT, usług ICT lub procesów ICT. Wyróżnia się następujące poziomy uzasadnienia zaufania:

1) podstawowy;
2) istotny;
3) wysoki.

2. Krajowy poziom uzasadnienia zaufania:

1) podstawowy – potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa lub wydana została krajowa deklaracja zgodności, spełniają odpowiadające im wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych podstawowych ryzyk w zakresie incydentów i cyberataków;
2) istotny – potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych ryzyk wystąpienia incydentów i cyberataków przeprowadzanych przez osoby dysponujące niezaawansowanym sprzętem oraz podstawowymi umiejętnościami w zakresie przełamywania zabezpieczeń systemów informacyjnych;
3) wysoki – potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach w zakresie przełamywania zabezpieczeń systemów informacyjnych lub dysponujące zawansowanym sprzętem.

3. Minimalne działania w zakresie oceny danego produktu ICT, usługi ICT czy procesu ICT obejmują:

1) w przypadku krajowego poziomu uzasadnienia zaufania ”podstawowy” – przegląd dokumentacji technicznej lub działania o równoważnym skutku,
2) w przypadku krajowego poziomu uzasadnienia zaufania ”istotny” – sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności oraz testowanie w celu wykazania, że w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne funkcjonalności bezpieczeństwa lub działania o równoważnym skutku,
3) w przypadku krajowego poziomu uzasadnienia zaufania ”wysoki” –obejmują sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności, testowanie, czy w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne, nowoczesne funkcjonalności bezpieczeństwa oraz ocenę sprawdzającą za pomocą testów penetracyjnych ich odporność na zaawansowane atak lub działania o równoważnym skutku.

Art. 59h. 1. Oceny zgodności w zakresie cyberbezpieczeństwa dokonuje akredytowana jednostka oceniająca zgodność spełniająca wymogi określone w załączniku nr 1 do rozporządzenia 2019/881 oraz w krajowym programie certyfikacji cyberbezpieczeństwa lub europejskim programie certyfikacji cyberbezpieczeństwa.

2. Akredytacji jednostki oceniającej zgodność dokonuje Polskie Centrum Akredytacji.

3. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku.

4. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji niezwłocznie o udzielonej akredytacji z zakresu krajowych programów certyfikacji cyberbezpieczeństwa i europejskich programów certyfikacji cyberbezpieczeństwa.

5. Informacja o udzielonej akredytacji, o której mowa w ust. 2, zawiera:

1) oznaczenie podmiotu, któremu udzielono akredytacji;
2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji.

6. Akredytacji udziela się na okres nie dłuższy niż 5 lat.

7. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji niezwłocznie o cofnięciu akredytacji jednostce oceniającej zgodność.

8. Informacja o cofnięciu akredytacji jednostce oceniającej zgodność zawiera:

1) oznaczenie podmiotu, któremu cofnięto akredytację;
2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji;
3) wskazanie daty cofnięcia akredytacji.

Art. 59i. 1. W przypadku, gdy:

1) europejski program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881,
2) krajowy program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi, o których mowa w art. 59f ust. 2 pkt 4

– czynności w ramach oceny zgodności dokonywanej na ich podstawie dokonuje tylko jednostka oceniająca zgodność posiadająca zezwolenie ministra do spraw informatyzacji.

2. Minister właściwy do spraw informatyzacji, w drodze decyzji, zezwala na wykonywanie przez jednostkę oceniającą zgodność zadań w ramach programów certyfikacji cyberbezpieczeństwa, o których mowa w ust. 1, na wniosek jednostki oceniającej zgodność, która spełniła wymogi określone w tych programach.

3. Minister właściwy do spraw informatyzacji może z urzędu cofnąć, ograniczyć albo zawiesić zezwolenie, o którym mowa w ust. 1, jeśli podmiot naruszył postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa albo krajowego programu certyfikacji cyberbezpieczeństwa. Cofnięcie, ograniczenie albo zawieszenie zezwolenia następuje w drodze decyzji.

4. Do postępowań o których mowa w ust. 2 stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego.

Art. 59j. 1. Produkt ICT, usługa ICT lub proces ICT może być poddany ocenie zgodności.

2. Ocena zgodności jest dobrowolna.

3. Warunki techniczne przeprowadzania oceny zgodności określają europejskie programy certyfikacji cyberbezpieczeństwa lub krajowe programy certyfikacji cyberbezpieczeństwa.

Art. 59k. Podczas dokonywania oceny zgodności produkt ICT, usługę ICT lub proces ICT poddaje się przed wydaniem:

1) deklaracji zgodności – badaniom przez dostawcę sprzętu lub oprogramowania, jeżeli nie jest wymagane przeprowadzenie badań przez laboratorium niezależne od dostawcy i odbiorcy;

2) certyfikatu –ocenie zgodności przez jednostkę oceniającą zgodność, w zakresie właściwym do danego programu certyfikacji cyberbezpieczeństwa.

Art. 59l. 1. Wniosek o certyfikację produktu ICT, usługi ICT lub procesu ICT składa jego dostawca do jednostki oceniającej zgodność.

2. Wniosek o certyfikację zawiera co najmniej:

1) nazwę albo imię i nazwisko wnioskującego oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania;
2) informacje potwierdzające spełnianie kryteriów certyfikacji;
3) wskazanie zakresu wnioskowanej certyfikacji.

3. Do wniosku dołącza się dokumenty potwierdzające spełnianie wymagań określonych we właściwym programie certyfikacyjnym.

4. Wniosek składa się pisemnie w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

Art. 59m. Jednostka oceniająca zgodność niezwłocznie przekazuje ministrowi właściwemu do spraw informatyzacji dane podmiotu, któremu wydano certyfikat, albo podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jego cofnięcia.

Art. 59n. 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji przesyła, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 2 ustawy z dnia 7 października 2020 r. o doręczeniach elektronicznych (Dz. U. poz. 2320, z późn. zm[4)]) do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego:

1) w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania „wysoki”;
2) w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania „wysoki”.

2. Minister właściwy do spraw informatyzacji:

1) zatwierdza certyfikat, o którym mowa w ust. 1;

[4)] Zmiany wymienionej ustawy zostały ogłoszone w Dz. U. z 2021 r. poz. 72, 802, 1135, 1163 i 1598.

2) odmawia zatwierdzenia certyfikatu, o którym mowa w ust. 1, jeżeli certyfikat został wydany niezgodnie z ustawą, rozporządzeniem 2019/881 lub programami, o których mowa w ust. 1.

3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego europejskiego programu certyfikacji cyberbezpieczeństwa lub krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja.

4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg procesu oceny zgodności.

5. Minister właściwy do spraw informatyzacji cofa certyfikat, jeśli jest on niezgodny z ustawą, rozporządzeniem 2019/881, europejskim programem certyfikacji cyberbezpieczeństwa lub krajowym programem certyfikacji cyberbezpieczeństwa.

6. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji.

Art. 59o. W przypadku stwierdzenia, że podmiot ubiegający się o uzyskanie certyfikatu nie spełnia kryteriów oceny zgodności, jednostka oceniająca zgodność odmawia jej dokonania, wskazując brak spełnienia kryteriów certyfikacji.

Art. 59p. 1. Dokumentem potwierdzającym certyfikację jest certyfikat.

2. Certyfikat zawiera co najmniej:

1) oznaczenie podmiotu, który otrzymał certyfikat;
2) nazwę podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby;
3) oznaczenie produktu ICT, usługi ICT lub procesu ICT podlegającego certyfikacji;
4) numer lub oznaczenie certyfikatu;
5) zakres certyfikacji;
6) okres, na jaki została dokonana certyfikacja;
7) wskazanie poziomu uzasadnienia zaufania określonego w europejskim programie certyfikacji cyberbezpieczeństwa lub krajowego poziomu uzasadnienia zaufania określonego w krajowym programie certyfikacji cyberbezpieczeństwa;
8) datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej.

3. Certyfikat, wydany w ramach krajowego programu certyfikacji cyberbezpieczeństwa, odwołuje się do związanych z produktem ICT, usługą ICT lub procesem ICT specyfikacji technicznych, norm i procedur, w tym kontroli technicznych

mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom.

4. Okres ważności krajowych certyfikatów cyberbezpieczeństwa określany jest na podstawie charakterystyki specyfikacji technicznej dla konkretnych produktów ICT, usług ICT lub procesów ICT.

Art. 59q. 1. W okresie, na jaki został wydany certyfikat, podmiot, któremu go wydano, jest obowiązany spełniać kryteria obowiązujące na dzień jego wydania.

2. Jednostka oceniająca zgodność cofa certyfikat w przypadku stwierdzenia, że podmiot, któremu wydano certyfikat nie spełnia lub przestał spełniać kryteria certyfikacji.

3. Jednostka oceniająca zgodność informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu certyfikatu na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 7 października 2020 r. o doręczeniach elektronicznych.

Art. 59r. 1. Dostawca, który poddał produkt ICT, usługę ICT lub proces ICT ocenie zgodności z zasadniczymi wymaganiami określonymi w krajowym programie certyfikacji cyberbezpieczeństwa i potwierdził ich zgodność, wydaje krajową deklarację zgodności.

2. Krajowa deklaracja zgodności, odwołuje się do określonych w krajowym programie certyfikacji cyberbezpieczeństwa specyfikacji technicznych, norm i procedur, w tym kontroli technicznych mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom.

3. Produkt ICT, usługa ICT lub proces ICT spełniają wymagania określone w programie certyfikacji przez cały okres na jaki została wydana deklaracja zgodności.

4. Krajowa deklaracja zgodności wydawana jest wyłącznie dla produktów ICT, usług ICT lub procesów ICT odpowiadających wymaganiom dla krajowego poziomu uzasadnienia zaufania „podstawowy”.

Art. 59s. Po wydaniu deklaracji zgodności dostawca przesyła jej kopię ministrowi właściwemu do spraw informatyzacji, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 7 października 2020 r. o doręczeniach elektronicznych.

Art. 59t. Domniemywa się, że wyrób, dla którego wydano deklarację zgodności jest zgodny z wymaganiami określonymi w obowiązujących krajowych programach certyfikacji cyberbezpieczeństwa lub europejskich programach certyfikacji cyberbezpieczeństwa.

Art. 59u. 1. Dostawca produktów ICT, usług ICT lub procesów ICT, posiadających krajowy certyfikat cyberbezpieczeństwa produktów ICT, usług ICT lub procesów IT, dla których została wydana krajowa deklaracja zgodności, udostępnia publicznie informacje zawierające:

1) porady i zalecenia mające pomóc użytkownikom końcowym w bezpiecznej: konfiguracji, instalacji i obsłudze oraz w bezpiecznym uruchomieniu i utrzymaniu produktów ICT, usług ICT lub procesów ICT;
2) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem;
3) informacje kontaktowe wytwórcy lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatnościach pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa;
4) odesłanie do repozytoriów internetowych zawierających wykaz podanych do wiadomości publicznej podatnościach związanych z produktami ICT, usługami ICT lub procesami ICT oraz innych poradników dotyczących cyberbezpieczeństwa.

2. Informacje, o których mowa w ust. 1, są aktualizowane co najmniej do czasu wygaśnięcia certyfikatu lub deklaracji zgodności.

Art. 59v. Podmiot, o którym mowa w art. 59a ust. 1 pkt 3 i 4, na wniosek ministra właściwego do spraw informatyzacji, przedstawia informacje dotyczące:

1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany certyfikat lub deklaracja zgodności;
2) funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa;
3) liczby wydanych certyfikatów, w tym programów w ramach których zostały wydane oraz poziomów uzasadnienia zaufania do których się odwoływały;
4) liczby wydanych deklaracji zgodności, w tym programów w ramach których zostały wydane;
5) liczby i sposobu rozpatrzenia skarg, o których mowa w art. 59y.

Art. 59w. 1. Minister właściwy do spraw informatyzacji, w ramach nadzoru, o którym mowa w art. 59a ust. 2, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów ICT, usług ICT lub procesów ICT.

2. Do kontroli, o której mowa w ust. 1, realizowanej wobec podmiotów:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców;

2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.

Art. 59x. Do kontroli, przeprowadzanej u przedsiębiorców, w ramach krajowego systemu certyfikacji cyberbezpieczeństwa przepisy art. 55-59 stosuje się.

Art. 59y. 1. Jednostki oceniające zgodność publikują na swojej stronie internetowej informacje o procedurze postępowania ze skargami, o których mowa w art. 63 rozporządzenia 2019/881. Procedura rozpatrywania skarg określa termin załatwienia skargi oraz przebieg procesu jej rozpatrywania.

2. Skargę składa się do jednostki oceniającej zgodność w terminie 14 dni od dnia doręczenia rozstrzygnięcia. Jednostka oceniające zgodność mogą określić dłuższy termin na złożenie skargi.

3. Jednostka oceniająca zgodność rozpatruje skargę w terminie nie dłuższym niż 2 miesiące.

4. Skargę rozpatrują osoby, które nie brały udziału w podejmowaniu rozstrzygnięcia, którego dotyczy skarga.

5. Jednostka oceniająca zgodność informuje skarżącego o stanie postępowania oraz o prawie skierowania sprawy do sądu na jego wniosek.

Art. 59z. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na:

1) podmiot, który wydał unijną lub krajową deklarację zgodności, jeśli produkt ICT, usługa ICT lub proces ICT, którego dana deklaracja dotyczy nie spełnia wymogów określonych w programie certyfikacji cyberbezpieczeństwa,

2) jednostkę oceniającą zgodność.

2. Do skarg, o których mowa w ust. 1, stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego.”;

44) w art. 62 w ust. 1:

a) w pkt 1 i 2 wyrazy „CSIRT MON, CSIRT NASK i CSIRT GOV" zastępuje się wyrazami "CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT i CSIRT sektorowy";

b) w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:

„7) wydawanie ostrzeżeń.”;

45) po art. 62 dodaje się art. 62a i 62b w brzmieniu:

„1. Dodatek do wynagrodzenia za pracę lub dodatek do uposażenia, zwane dalej „świadczeniem teleinformatycznym'', przysługuje osobom albo funkcjonariuszom realizującym zadania:

1) o których mowa w art. 26, art. 36b, art. 42 ust. 1, art. 44, w art. 44a ust. 3 i art. 62

2) w zakresie zapewnienia cyberbezpieczeństwa w:

a) Centralnym Biurze Antykorupcyjnym,

b) Kancelarii Prezesa Rady Ministra oraz urzędach obsługujących ministrów,

c) Policji,

d) prokuraturze,

e) Służbie Kontrwywiadu Wojskowego,

f) Służbie Wywiadu Wojskowego,

g) Straży Granicznej.

2. W przypadku funkcjonariuszy świadczenie teleinformatyczne stanowi dodatek do uposażenia, o którym mowa odpowiednio w:

1) ustawie z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2020 r. poz. 360 z późn. zm.[5]);

2) ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2021 r. poz. 1486 i 1728).

3) ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27 i 2320);

4) ustawie z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz. U. z 2021 r. poz. 1131 i 1666);

5) ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2021 r. poz. 1671);

6) ustawie z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz. U. z 2021 r. poz. 1362);

7) ustawie z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2021 r. poz. 575 i 1728);

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2020 r. poz. 956, 1610, 2112 i 2320 oraz z 2021 r. poz.1005 i 1728.

3. Wysokość wynagrodzenia za pracę albo uposażenia z uwzględnieniem świadczenia teleinformatycznego wynosi do dwudziestojednokrotności kwoty bazowej dla członków korpusu służby cywilnej, ustalanej w ustawie budżetowej.

4. Świadczenie teleinformatyczne jest przyznawane na okres realizacji zadań, o których mowa w ust. 1.

5. Przyznania i cofnięcia świadczenia teleinformatycznego dokonuje kierownik urzędu, w którym są zatrudnione osoby albo pełnią służbę funkcjonariusze, o których mowa w ust. 1.

6. Do przyznawania i cofania świadczenia teleinformatycznego nie stosuje się przepisów ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2020 r. poz. 1320 oraz z 2021 r. poz. 1162) dotyczących wypowiadania warunków pracy lub płacy.

7. Osobie, o której mowa w ust. 1, cofa się świadczenie teleinformatyczne w przypadku:

1) ukarania karą porządkową albo dyscyplinarną;
2) nieusprawiedliwionej nieobecności w pracy, trwającej co najmniej 2 dni;
3) stawienia się do pracy w stanie nietrzeźwym lub wskazującym na spożycie alkoholu albo pod wpływem środków odurzających;
4) spożywania alkoholu lub używania środków odurzających w czasie pracy;
5) opuszczenia miejsca pracy bez usprawiedliwienia;
6) odmowy wykonania polecenia lub niewykonania czynności wchodzących w zakres jego obowiązków.

8. Ponowne ustalenie wysokości świadczenia teleinformatycznego, w przypadku zaistnienia okoliczności, o których mowa w ust. 7, nie może nastąpić wcześniej niż po upływie:

1) okresu 3 miesięcy – w przypadkach, o których mowa w ust. 7 pkt 2 lub 5;
2) okresu 6 miesięcy – w pozostałych przypadkach, o których mowa w ust. 7, innych niż wskazane w ust. 7 pkt 2 lub 5.

9. Świadczenia teleinformatycznego nie wypłaca się za okres:

1) korzystania z urlopu bezpłatnego;
2) nieusprawiedliwionej nieobecności w pracy trwającej krócej niż 2 dni;
3) usprawiedliwionej nieobecności w pracy, z wyłączeniem urlopu wypoczynkowego, dodatkowego urlopu wypoczynkowego oraz urlopu okolicznościowego.

10. Świadczenie teleinformatyczne jest wypłacane w terminie płatności wynagrodzenia za pracę albo uposażenia.

11. W zakresie nieuregulowanym w ustawie stosuje się przepisy dotyczące zatrudnienia albo pełnienia służby stosowane odpowiednio w podmiotach, w których są zatrudnione albo pełnią służbę osoby, o których mowa w ust. 1.

12. Rada Ministrów określi, w drodze rozporządzenia:

1) podział na grupy zadań, o których mowa w ust. 1 ustawy, zwanych dalej ,,zadaniami z zakresu cyberbezpieczeństwa";
2) kwalifikacje zawodowe wymagane do realizacji zadań z poszczególnych grup oraz sposób ich weryfikacji przez kierownika właściwego podmiotu;
3) mnożnik do ustalenia wysokości dodatku do wynagrodzenia w związku z realizacją zadań z zakresu cyberbezpieczeństwa;
4) mnożnik do ustalenia wysokości dodatku do uposażenia w związku z realizacją zadań z zakresu cyberbezpieczeństwa.

– biorąc pod uwagę stawki rynkowe, plan finansowy Funduszu Cyberbezpieczeństwa oraz wymagania kwalifikacyjne określone dla osób realizujące podobne zadania na rynku.

13. Rada Ministrów może określić, w drodze rozporządzeniu, limit wydatków w zakresie dodatków, o których mowa w ust. 1, dla kierowników poszczególnych podmiotów, o których mowa w ust. 1, w danym roku budżetowym.

Art. 62b. 1. Pełnomocnik może wydawać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.

2. Rekomendacje Pełnomocnika są udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.

4. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.

5. Podmiot krajowego systemu cyberbezpieczeństwa, uwzględnia rekomendacje w zarządzaniu ryzykiem.”;

46) w art. 64 po wyrazach „CSIRT GOV,” dodaje się wyrazy „CSIRT INT,”;

47) w art. 65:

a) w ust. 1:

– w pkt 2 po wyrazach „CSIRT GOV,” dodaje się wyrazy „Szefa Agencji Wywiadu realizującego zadania w ramach CSIRT INT,”,

– w pkt 4 po wyrazach „Agencji Bezpieczeństwa Wewnętrznego” dodaje się wyrazy „ Szefa Agencji Wywiadu”;

– w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:

„7) decyzji o w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.”;

b) dodaje się ust. 3 w brzmieniu:

„3. Kolegium przyjmuje i rozpatruje sprawy na posiedzeniu albo może również rozpatrywać poszczególne sprawy w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).”;

48) po art. 64 dodaje się art. 64a w brzmieniu:

„Art. 64a. 1. Przewodniczący Kolegium może zlecić CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1, uwzględniającej informacje przekazane przez państwa członkowskie lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przekazane przez sektor prywatny.

2. Przewodniczący Kolegium może zlecić CSIRT GOV, CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT.

3. Zadania, o których mowa w ust. 1 i 2, są wykonywane w ramach ustawowych zadań odpowiednio CSIRT GOV, CSIRT MON lub CSIRT NASK.”;

49) w art. 66:

a) w ust. 1 pkt 4 otrzymuje brzmienie:

„4) członkowie Kolegium:

a) minister właściwy do spraw wewnętrznych,

b) minister właściwy do spraw informatyzacji,

c) minister właściwy do spraw energii,

d) Minister Obrony Narodowej,

e) minister właściwy do spraw zagranicznych,

f) Szef Kancelarii Prezesa Rady Ministrów,

g) Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej,

h) minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister - członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego,

i) Przewodniczący Komisji Nadzoru Finansowego,

j) kierownik państwowej jednostki budżetowej, właściwej w zakresie cyberbezpieczeństwa, podległej Ministrowi Obrony Narodowej lub przez niego nadzorowanej, jeżeli został wyznaczony przez Ministra Obrony Narodowej.”,

b) ust. 4 otrzymuje brzmienie:

„4. W posiedzeniach Kolegium uczestniczą również:

1) Dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;

2) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca;

3) Szef Agencji Wywiadu albo jego zastępca;

4) Szef Centralnego Biura Antykorupcyjnego albo jego zastępca;

5) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca;

6) Szef Służby Wywiadu Wojskowego albo jego zastępca;

7) Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego albo jego zastępca.”;

c) w ust. 5 po pkt. 2, kropkę zastępuje się średnikiem i dodaje się pkt 3-8 w brzmieniu:

„3) może pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;

4) może zlecić CSIRT GOV, CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1;

5) może zlecić CSIRT GOV, CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2;

6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1;

7) powołuje zespół opiniujący, o którym mowa w art. 66a ust. 10 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład.;

8) rozstrzyga spór, o którym mowa w art. 66a ust. 10 pkt 2, wskazując właściwego członka zespołu opiniującego.";

d) w ust. 7 po wyrazach „CSIRT NASK,” dodaje się wyrazy „CSIRT INT,”;

50) po art. 66 dodaje się art. 66a-art. 66e w brzmieniu:

„Art. 66a. 1. Minister właściwy do spraw informatyzacji, w celu ochrony ważnego interesu państwowego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania za dostawcę wysokiego ryzyka dostawcy sprzętu lub oprogramowania, które jest wykorzystywane przez:

1) podmioty krajowego systemu cyberbezpieczeństwa,

2) przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń,

3) właścicieli lub posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,

4) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców,

– zwane dalej „postępowaniem w sprawie uznania za dostawcę wysokiego ryzyka”.

2. Dostawcą sprzętu lub oprogramowania, o którym mowa w ust. 1, jest dostawca produktów ICT, usług ICT lub procesów ICT.

3. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka stosuje się, jeżeli ustawa nie stanowi inaczej, przepisy ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy.

4. Stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.

5. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

6. Zawiadomienie, o którym mowa w ust. 5, udostępnia się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) - stronie umowy o Europejskim Obszarze Gospodarczym. Udostępnienie ma skutek doręczenia po upływie 14 dni od dnia jego dokonania.

7. W przypadku wszczęcia postępowania w sprawie uznania za dostawcę wysokiego ryzyka z urzędu, minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Terminu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego nie stosuje się.

8. Opinia, o której mowa w ust. 7 zdanie pierwsze, zawiera analizę:

1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego;
2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:
   a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie,
   b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności tam gdzie nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,
   c) struktury własnościowej dostawcy sprzętu lub oprogramowania,
   d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;
3) trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z

dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.5.2019, str. 1-12, z późn. zm.);

4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;
5) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt 1-4, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
6) treści wydanych wcześniej rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy.

9. Sporządzając opinię, o której mowa w ust. 7, Kolegium uwzględnia:

1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;
2) analizę, o której mowa w art. 64a ust. 1 i 2, jeżeli przewodniczący Kolegium zleciło jej przeprowadzenie.

10. Procedura sporządzenia opinii, o której mowa w ust. 7, przebiega w następujący sposób:

1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzą przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium;
2) każdy członek zespołu opiniującego przygotowuje stanowisko, w zakresie swojej właściwości, na podstawie analizy określony w ust. 8, które następnie przekazuje zespołowi, o którym mowa w pkt 1. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium wskazując właściwego członka zespołu opiniującego;
3) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;
4) uzgodnienie opinii następuje na posiedzeniu Kolegium;

5) uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

11. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.

12. Decyzja, o której mowa w ust. 11, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka.

13. Minister właściwy do spraw informatyzacji ogłasza decyzję, o której mowa w ust. 11, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz udostępnia na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra.

14. Decyzja, o której mowa w ust. 11, podlega natychmiastowemu wykonaniu.

15. Od decyzji, o której mowa w ust. 11, nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Art. 66b. 1. W przypadku wydania decyzji, o której mowa w art. 66a ust. 11, podmioty, o których mowa w art. 66a ust. 1 pkt 1-4:

1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;
2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 11.

2. Przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, wycofują w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.

3. Podmioty, o których mowa w art. 66 ust. 1 pkt 1-4, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129 i 1598), nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 11.

Art. 66c. 1. Podmioty krajowego systemu cyberbezpieczeństwa oraz przedsiębiorcy telekomunikacyjni są zobowiązani przekazać informacje na wniosek uprawnionych organów, o których mowa w ust. 2, o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją.

2. Uprawnionymi organami do żądania informacji, o których mowa w ust. 1, są wobec:

1) operatorów usług kluczowych i dostawców usług cyfrowych – organy właściwe do spraw cyberbezpieczeństwa;
2) SOC – minister właściwy do spraw informatyzacji;
3) przedsiębiorców telekomunikacyjnych – Prezes Urzędu Komunikacji Elektronicznej;
4) podmiotów publicznych – właściwe organy nadzorcze;
5) właściciele i posiadacze obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym - ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialnych za systemy, o których mowa w art. 3 pkt 2 ustawy z dnia 28 kwietnia 2007 r. o zarządzaniu kryzysowym;
6) przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców - organy administracji rządowej właściwe do organizowania oraz sprawowania nadzoru nad realizacją zadań na rzecz obronności państwa.

3. Wniosek zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę wydania;
3) wskazanie zakresu żądanych informacji;
4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
5) uzasadnienie.

4. Pełnomocnik może zwrócić się do organów, o których mowa w ust. 2, o żądanie informacji, o których mowa w ust. 1.

Art. 66d. 1. Sąd administracyjny rozpatruje skargę na decyzje, o której mowa w art. 66a ust. 11, na posiedzeniu niejawnym.

2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych.

3. Sąd administracyjny nie może wstrzymać wykonalności decyzji, o której mowa w art. 66a ust. 11, po wniesieniu skargi na tę decyzję.

Art. 66e. Minister właściwy do spraw informatyzacji prowadzi i udostępnia przy użyciu systemu teleinformatycznego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 66a ust. 11.”;

51) w art. 67 w ust. 1 po pkt 3 dodaje się pkt 3a w brzmieniu:

„3a) Szefa Agencji Wywiadu - w odniesieniu do działalności CSIRT INT;”;

52) po art. 67 dodaje się art. 67a-67e w brzmieniu:

„Art. 67a. 1. Pełnomocnik w przypadku uzyskania informacji wskazującej na możliwość wystąpienia incydentu krytycznego, może wydać ostrzeżenie w celu poinformowania o cyberzagrożeniu:

1) podmiotów, o których mowa w art. 4 pkt 1–16;
2) przedsiębiorców telekomunikacyjnych;
3) właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
4) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców;
5) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2020 r. poz. 794 i 1639 oraz z 2021 r. poz. 355, 1598 i 1814);
6) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w

odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

2. Pełnomocnik, przed wydaniem ostrzeżenia, przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę uzasadniającą jego wydanie obejmującą:

1) istotność cyberzagrożenia;
2) prawdopodobieństwo wystąpienia incydentu krytycznego;
3) rodzaje ryzyk;
4) skuteczność alternatywnych metod zapewnienia cyberbezpieczeństwa.

3. Ostrzeżenie zawiera:

1) wskazanie rodzajów ryzyk;
2) wskazanie rodzajów podmiotów, których dotyczy;
3) zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu;
4) datę wejścia w życie;
5) uzasadnienie zawierające wyniki analizy, o której mowa w ust. 2.

4. Pełnomocnik przeprowadza nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. W ramach przeglądu ostrzeżeń Pełnomocnik może przeprowadzić analizę, o której mowa w ust. 2. Pełnomocnik po uzyskaniu informacji o ustaniu zagrożenia wystąpienia incydentu krytycznego odwołuje ostrzeżenie.

5. Pełnomocnik udostępnia:

1) informację o wydanym ostrzeżeniu, a także o odwołaniu ostrzeżenia,
2) listę wydanych i odwołanych ostrzeżeń

– w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika, a także na stronie internetowej urzędu obsługującego Pełnomocnika.

6. Jeżeli przemawia za tym interes publiczny, informacja o wydaniu ostrzeżenia może być udostępniona za pomocą środków masowego przekazu.

7. Informacja o wydaniu ostrzeżenia może być przekazana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

8. Przez zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu krytycznego, rozumie się zalecenie:

1) przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;
2) dokonania przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu związanego z daną podatnością;
3) wdrożenia określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność;
4) dokonania określonej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności;
5) prowadzenia wzmożonego monitorowania zachowania systemu;
6) odstąpienia od korzystania z określonego sprzętu lub oprogramowania;
7) wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL.

9. Operator usługi kluczowej uwzględnia wydane ostrzeżenia podczas procesu szacowania ryzyka.

Art. 67b. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające.

2. Polecenie zabezpieczające dotyczy nieokreślonej liczby:

1) podmiotów, o których mowa w art. 4 pkt 1–16;
2) przedsiębiorców telekomunikacyjnych;
3) właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
4) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców;
5) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych;
6) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego stosuje się odpowiednio przepisy ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, z wyjątkiem przepisów art. 10, art. 34, art. 81, art. 81a, art. 107 § 1 pkt 3, 145 § 1 pkt 4 i 156 § 1 pkt 4.

4. Stronę zawiadamia się o czynnościach w sprawie przez publiczne udostępnienie informacji na stronie podmiotowej ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej.

5. Minister właściwy do spraw informatyzacji, przed wydaniem polecenia zabezpieczającego przeprowadza, we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę uzasadniającą jego wydanie, obejmującą:

1) istotność cyberzagrożenia;
2) przewidywane, potencjalne skutki incydentu krytycznego;
3) rodzaje ryzyk;
4) skutki finansowe, społeczne i prawne wydania polecenia zabezpieczającego.

6. Polecenie zabezpieczające zawiera:

1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy;
2) obowiązek określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się oraz termin jego wdrożenia.

7. Przez zachowanie, o którym mowa w ust. 6 pkt 2, rozumie się:

1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk,
2) nakaz przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu związanego z daną podatnością,
3) nakaz zastosowania określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność,
4) nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności,
5) nakaz wzmożonego monitorowania zachowania systemu,
6) zakaz korzystania z określonego sprzętu lub oprogramowania,
7) nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu określonego w art. 67b ust. 1, który skutkując zakłóceniem usług świadczonych przez ten podmiot został

sklasyfikowany przez właściwy CSIRT GOV, CSIRT MON lub CSIRT NASK jako przyczyna trwającego incydentu krytycznego,

8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania,

9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych, lub

10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

8. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 6 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 4.

9. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata.

10. Polecenie zabezpieczające wygasa:

1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub

2) po upływie czasu na które zostało wydane.

11. Polecenie zabezpieczające podlega natychmiastowej wykonalności.

12. Minister właściwy do spraw informatyzacji ogłasza polecenie zabezpieczające w dzienniku urzędowym ministra właściwego do spraw informatyzacji. Informacje o poleceniu zabezpieczającym udostępnia się również na stronie podmiotowej ministra w Biuletynie Informacji Publicznej lub na stronie internetowej urzędu obsługującego ministra.

13. Polecenie zabezpieczające uznaje się za doręczone z chwilą ogłoszenia polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

14. Od decyzji, o której mowa w ust. 1, nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Art. 67c. 1. Skargę na polecenie zabezpieczające wnosi się w terminie 2 miesięcy od dnia, w którym polecenie zabezpieczające zostało ogłoszone.

2. Sąd administracyjny zarządza połączenie wszystkich oddzielnych spraw toczących się przed nim w celu ich łącznego rozpoznania i rozstrzygnięcia, jeżeli dotyczą tego samego polecenia zabezpieczającego.

3. Wniosek o przywrócenie terminu na złożenie skargi jest niedopuszczalny.

Art. 67d 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 66b i art. 66c oraz art. 67b.

2. Minister właściwy do spraw informatyzacji przekazuje niezwłocznie Prezesowi Narodowego Banku Polskiego informacje o:

1) decyzjach wydanych na podstawie art. 66a ust. 12;
2) wydanych poleceniach zabezpieczających.

Art. 67e. 1. Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może podjąć decyzję o czasowym powierzeniu temu ministrowi realizacji wybranych zadań, o których mowa w art. 26 ustawy.

2. Decyzja, o której mowa w ust. 1, określa w szczególności:

1) zakres powierzonych zadań;
2) czas realizacji powierzonych zadań lub sposób ich odwołania;
3) w razie potrzeby - szczególne zasady współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV;
4) zasady informowania Kolegium o stanie realizacji powierzonych zadań.

3. Realizacja zadań, o których mowa w ust. 1, dokonywana jest przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych.”;

53) po art. 72 dodaje się rozdział 13a w brzmieniu:

„Rozdział 13a

Fundusz Cyberbezpieczeństwa

Art. 72a. 1. Fundusz Cyberbezpieczeństwa, zwany dalej „Funduszem”, jest państwowym funduszem celowym.

2. Dysponentem Funduszu jest minister właściwy do spraw informatyzacji.

3. Przychodami Funduszu są:

1) dotacje z budżetu państwa;
2) wpływy z kar pieniężnych, o których mowa w art. 73, 75 i 75a;
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) środki, o których mowa w ust. 5;

6) inne przychody.

4. Kosztami Funduszu są:

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

5. Dyrektor Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego może, w drodze porozumienia z ministrem właściwym do spraw informatyzacji, przekazać część środków z planu finansowego tego instytutu, w tym z wypracowanego przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy zysku netto za poprzedni rok obrotowy, do Funduszu z przeznaczeniem na sfinansowanie jego kosztów.

6. Warunkiem ubiegania się o wsparcie ze środków Funduszu w zakresie, o którym mowa w ust. 4 pkt 1, jest złożenie do ministra właściwego do spraw informatyzacji wniosku zawierającego szczegółowy opis zadań wraz z liczbą osób wykonującym dane zadania oraz oświadczeniem kierownika podmiotu o spełnieniu wymagań określonych w rozporządzeniu, o którym mowa w art. 62a ust. 12a.

7. Wsparcia ze środków Funduszu w zakresie, o którym mowa w ust. 4 pkt 2, udziela się w drodze otwartego i niedyskryminacyjnego naboru wniosków o udzielenie wsparcia.

8. Warunkiem ubiegania się o wsparcie ze środków Funduszu, o którym mowa w ust. 7, jest spełnienie wymagań określonych każdorazowo dla danego naboru wniosków o udzielenie wsparcia.

9. Warunkiem ubiegania się o wsparcie ze środków Funduszu, o którym jest mowa w ust. 4 pkt 3, jest złożenie wniosku do ministra właściwego do spraw informatyzacji, zawierającego szczegółowy opis działań związanych ze zwiększeniem poziomu cyberbezpieczeństwa systemów infrastruktury krytyczne wraz z terminem ich realizacji oraz kosztorysami. W przypadku decyzji o udzieleniu wsparcia przez dysponenta Funduszu, do przekazania środków z Funduszu , do części budżetowej ubiegającego się o wsparcie ze środków Funduszu niezbędna jest uchwała Rady Ministrów.

Art. 72b 1. Dofinansowanie realizacji zadań o których mowa w art. 72a ust. 4 pkt 2 ze środków Funduszu , odbywa się na wniosek zainteresowanego podmiotu.

2. Dofinansowanie następuje w formie dotacji celowej ze środków Funduszu ,.

3. Wniosek o dofinansowanie zawiera w szczególności:

1) nazwę (firmę) wnioskodawcy;
2) tytuł lub nazwę wniosku;
3) harmonogram realizacji projektu objętego wnioskiem;
4) opis projektu objętego wnioskiem i jej lokalizacji;
5) opis spełniania kryteriów oceny wniosków;
6) wartość kosztorysową projektu;
7) kwotę wnioskowanej dotacji celowej;
8) proponowany procent dofinansowania projektu;
9) proponowaną kwotę dofinansowania w podziale na poszczególne lata realizacji projektu;
10) określenie wysokości środków własnych wnioskodawcy lub środków przeznaczonych na realizację projektu uzyskanych od innych podmiotów, wraz ze wskazaniem tych podmiotów, oraz opis spodziewanych korzyści z realizacji projektu;
11) informację o wymaganiach w zakresie zasobów rzeczowych i zasobów kadrowych oraz kompetencji osób, zapewniających prawidłową realizację projektu.

Art. 72c. 1. Wybór wniosków o dofinansowanie działań o których mowa w art. 72a ust. 4 pkt 2, następuje w drodze konkursu.

2. W przypadku gdy kwota przeznaczona w konkursie na dofinansowanie jest wystarczająca do objęcia dofinansowaniem wszystkich wniosków, o których mowa w ust. 1, dofinansowanie mogą uzyskać wnioski, które spełniły kryteria oceny wniosków.

3. W przypadku gdy kwota przeznaczona w konkursie na dofinansowanie nie jest wystarczająca do objęcia dofinansowaniem wszystkich wniosków, o których mowa w ust. 1, dofinansowanie mogą uzyskać wnioski, które spełniły kryteria oceny wniosków i uzyskały:

1) wymaganą liczbę punktów albo
2) kolejno największą liczbę punktów.

Art. 72d. 1. Ogłoszenie o konkursie, o którym mowa w art. 72c, minister właściwy do spraw informatyzacji podaje do publicznej wiadomości przez publikację na stronie

internetowej urzędu obsługującego ministra właściwego do spraw informatyzacji oraz w Biuletynie Informacji Publicznej tego urzędu, co najmniej 30 dni przed rozpoczęciem konkursu.

2. Ogłoszenie o konkursie zawiera:

1) określenie przedmiotu konkursu;
2) określenie kwoty przeznaczonej na dofinansowanie wniosków;
3) określenie maksymalnego dopuszczalnego poziomu dofinansowania wniosku lub maksymalnej dopuszczalnej kwoty dofinansowania wniosku;
4) termin i formę składania wniosków o dofinansowanie.

Art. 72e. 1. Minister właściwy do spraw informatyzacji organizuje i przeprowadza konkurs, o którym mowa w art. 72c na podstawie określonego przez siebie regulaminu.

2. Regulamin konkursu określa:

1) przedmiot konkursu;
2) termin i formę składania wniosków o dofinansowanie i sposób uzupełniania braków formalnych oraz poprawiania oczywistych omyłek;
3) wzór wniosku o dofinansowanie ze środków dotacji celowej;
4) wzór umowy o dofinansowanie ze środków dotacji celowej;
5) czynności, jakie wnioskodawca jest obowiązany dokonać przed zawarciem umowy o dofinansowanie ze środków dotacji celowej, oraz wymagane dokumenty i terminy ich przedłożenia ministrowi właściwemu do spraw informatyzacji;
6) kryteria oceny wniosków wraz z określeniem ich znaczenia;
7) zakres, w jakim jest możliwe uzupełnianie lub poprawianie wniosku w części dotyczącej spełniania przez wniosek kryteriów oceny wniosków w trakcie oceny wniosku;
8) formę i sposób komunikacji między wnioskodawcą a ministrem właściwym do spraw informatyzacji, w tym wzywania wnioskodawcy do uzupełniania lub poprawiania wniosku, w trakcie jego oceny, w części dotyczącej spełniania kryteriów oceny, o których mowa w pkt 7, a także informację o skutkach niezachowania wskazanej formy i wskazanego sposobu komunikacji;
9) kwotę dotacji celowej przeznaczonej na dofinansowanie wniosków wraz z informacją dotyczącą możliwości jej zwiększenia;
10) maksymalną dopuszczalną kwotę dotacji celowej;
11) informację dotyczącą środków odwoławczych;

12) sposób podania do publicznej wiadomości wyników konkursu;
13) formę i sposób udzielania wyjaśnień w sprawach dotyczących konkursu;
14) informację w zakresie możliwości skrócenia terminu składania wniosków o dofinansowanie.

3. Do czasu rozstrzygnięcia konkursu, o którym mowa w art. 72c, minister właściwy do spraw informatyzacji nie może zmieniać regulaminu konkursu w sposób skutkujący nierównym traktowaniem wnioskodawców.

4. Przepisu ust. 3 nie stosuje się, jeżeli konieczność dokonania zmiany regulaminu konkursu wynika z odrębnych przepisów.

5. Minister właściwy do spraw informatyzacji podaje do publicznej wiadomości na stronie internetowej urzędu obsługującego ministra właściwego do spraw zdrowia oraz w Biuletynie Informacji Publicznej tego urzędu, regulamin konkursu oraz jego zmiany, wraz z ich uzasadnieniem i terminem, od którego są stosowane.

Art. 72f. Termin składania wniosków o dofinansowanie w konkursie, o którym mowa w art. 72c, nie może być krótszy niż 7 dni, licząc od dnia rozpoczęcia konkursu.

Art. 72g. 1. W razie stwierdzenia braków formalnych we wniosku o dofinansowanie, minister właściwy do spraw informatyzacji wzywa wnioskodawcę do uzupełnienia wniosku w wyznaczonym terminie, nie krótszym niż 7 dni i nie dłuższym niż 21 dni, pod rygorem pozostawienia wniosku bez rozpatrzenia.

2. W razie stwierdzenia oczywistej omyłki we wniosku o dofinansowanie, minister właściwy do spraw informatyzacji poprawia tę omyłkę z urzędu, informując o tym wnioskodawcę, albo wzywa wnioskodawcę do poprawienia oczywistej omyłki w wyznaczonym terminie, nie krótszym niż 7 dni i nie dłuższym niż 21 dni, pod rygorem pozostawienia wniosku bez rozpatrzenia.

3. W razie złożenia wniosku o dofinansowanie po terminie wskazanym w ogłoszeniu o konkursie, wniosek pozostawia się bez rozpatrzenia. Wniosek pozostawia się bez rozpatrzenia także w przypadku niezachowania formy i sposobu komunikacji określonych w regulaminie konkursu.

Art. 72h. 1. Minister właściwy do spraw informatyzacji dokonuje oceny wniosków o dofinansowanie na podstawie kryteriów, o których mowa w art. 72e ust. 1 pkt 6.

2. Minister właściwy do spraw informatyzacji, po zakończeniu oceny wniosków, przygotowuje i zatwierdza listę rankingową zawierającą wnioski objęte dofinasowaniem.

3. Lista rankingowa zawiera:

1) wnioski uszeregowane pod względem liczby przyznanych punktów w kolejności od największej do najmniejszej;
2) nazwę (firmę) wnioskodawcy,
3) tytuł albo nazwę wniosku;
4) przewidywany okres realizacji wniosku;
5) wartość kosztorysową wniosku;
6) kwotę wnioskowanej dotacji celowej;
7) proponowany procent dofinansowania wniosku;
8) proponowaną kwotę dofinansowania w podziale na poszczególne lata realizacji wniosku.

4. Na liście rankingowej uwzględnia się wszystkie wnioski, które podlegały ocenie.

5. Minister właściwy do spraw informatyzacji podaje listę rankingową do publicznej wiadomości na stronie internetowej urzędu obsługującego tego ministra oraz w Biuletynie Informacji Publicznej tego urzędu.

Art. 72i. Wnioskodawcy nie przysługuje prawo wniesienia wniosku o dokonanie ponownej oceny wniosku o dofinansowanie w przypadku, gdy proponowany procent dofinansowania wniosku, o którym mowa w art. 72h ust. 3 pkt 7, wynosi 0.

Art. 72j. Do postępowania w zakresie konkursu, o którym mowa w art. 72c, nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyjątkiem przepisów dotyczących obliczania terminów oraz wyłączenia pracownika i organu.

53) w art. 73:

a) w ust. 1
   – w pkt 4 wyraz „osoby” zastępuje się wyrazem „osób”,
   – w pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 i 15 w brzmieniu:
   „14) nie korzysta z systemu, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11;
   15) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 3.”;

b) po ust. 1 dodaje się ust. 1a-1c w brzmieniu:
   „1a. Jednostka oceniająca zgodność, która:
   1) nie przekazuje informacji, o których mowa w art. 59m i art. 59q ust. 3 lub przekazuje je nieprawdziwe lub niekompletne,
   2) nie wykonuje obowiązku określonego w art. 59y ust. 1 albo art. 59s

– podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotnego przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej za rok poprzedzający rok wymierzenia tej kary, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2021 r. poz. 291, 353, 794 i 1621), zwanego dalej „przeciętnym wynagrodzeniem”.

1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotnego przeciętnego wynagrodzenia.

1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która:

1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59w,
2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59w,
3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa,
4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji

– podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotnego przeciętnego wynagrodzenia.”,

c) po ust. 2 dodaje się ust. 2a-2c w brzmieniu:

„2a. Karze pieniężnej podlega podmiot określony w art. 66a ust. 1 pkt 1-4, który nie dostosował się do obowiązków określonych w art. 66b.

2b. Karze pieniężnej podlega podmiot, określony w art. 67b ust. 1, który nie dostosował się do polecenia zabezpieczającego.

2c. Karze pieniężnej podlega podmiot publiczny, który nie wyznaczył osób, o których mowa w art. 21.”,

d) w ust. 3:

– pkt 9 otrzymuje brzmienie:

„9) ust. 1 pkt 10 i 15, wynosi do 100 000 zł;”,

– po pkt 11 dodaje się pkt 11a w brzmieniu:

„11a) ust. 1 pkt 14 wynosi do 100 000 zł;”

– dodaje się pkt 14-16 w brzmieniu:

„14) ust. 2a, wynosi:

a) w przypadku podmiotów określonych w art. 66a ust. 1 pkt 1-4, z wyjątkiem podmiotów publicznych, w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,

b) w przypadku podmiotów publicznych do 100 000 zł;

15) ust. 2b, wynosi:

a) w przypadku podmiotów określonych w art. 67b ust. 1 z wyjątkiem podmiotów publicznych, w wysokości do 3% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego,

b) w przypadku podmiotów publicznych do 100 000 zł;

16) ust. 2c, wynosi do 10 000 zł.”,

e) dodaje się ust. 6 w brzmieniu:

6. Niezależnie od kary pieniężnej, o której mowa w ust. 2c, minister właściwy do spraw informatyzacji może nałożyć, w drodze decyzji, na kierującego podmiotem publicznym, o którym mowa w art. 4 pkt 7-15, realizującym zadanie publiczne zależne od systemu informacyjnego, karę pieniężną w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek,”;

54) w art. 74:

a) ust. 1 otrzymuje brzmienie:

„1. Karę pieniężną, o której mowa w art. 73 ust. 1 i 2, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.”,

b) dodaje się ust. 1a i 1b w brzmieniu:

„1a. Karę pieniężną, o której mowa w art. 73 ust. 1a-1c, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

1b. Karę pieniężną określoną w art. 73 ust. 2a-2c, nakłada w drodze decyzji minister właściwy do spraw informatyzacji.”;

55) po art. 75 dodaje się art. 75a w brzmieniu:

„Art. 75a. 1. Organ właściwy do spraw cyberbezpieczeństwa nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT sektorowego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 44 ust. 1a.

2. Szef Agencji Wywiadu nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT INT, jeżeli nie został wykonany obowiązek, o którym mowa w art. 36c.

3. Kara pieniężna, o której mowa w ust. 1 i 2, nakładana jest w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek.”;

56) przed art. 77 dodaje się oznaczenie i tytuł działu oraz oznaczenie i tytuł rozdziału w brzmieniu:

„DZIAŁ III. STRATEGICZNA SIEĆ BEZPIECZEŃSTWA

Rozdział 1

Operator strategicznej sieci bezpieczeństwa

Art. 76a. 1. W celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji, tworzy się strategiczną sieć bezpieczeństwa.

2. Strategiczna sieć bezpieczeństwa jest uruchamiana oraz zarządzana przez Operatora strategicznej sieci bezpieczeństwa.

Art. 76b. Prezes Rady Ministrów wyznacza Operatora strategicznej sieci bezpieczeństwa, w drodze zarządzenia, spośród podmiotów spełniających łącznie następujące warunki:

1) będących jednoosobową spółką Skarbu Państwa;
2) będących przedsiębiorcą telekomunikacyjnym;
3) posiadających infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w ust. 1;
4) posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej;
5) posiadających świadectwo bezpieczeństwa przemysłowego.

Art. 76c. 1. Operator strategicznej sieci bezpieczeństwa w celu realizacji zadań, o których mowa w ust. 1, świadczy usługi telekomunikacyjne oraz może świadczyć usługi

związane z zapewnieniem udogodnień towarzyszących oraz usług z zakresu cyberbezpieczeństwa.

2. Operator strategicznej sieci bezpieczeństwa może świadczyć usługi telekomunikacyjne także w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym w rozumieniu art. 111 ust. 2 pkt 2 i 3 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne. Wykorzystanie częstotliwości użytkowanych jako rządowe przez Operatora strategicznej sieci bezpieczeństwa koordynuje Minister Obrony Narodowej, z wyjątkiem ust. 3.

3. Wykorzystanie częstotliwości, o których mowa w art. 76o ust. 1, przez Operatora strategicznej sieci bezpieczeństwa koordynuje Prezes Urzędu Komunikacji Elektronicznej, zwany dalej „Prezesem UKE”. Przepisy art. 143 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stosuje się odpowiednio.

Art. 76d. 1. Operator strategicznej sieci bezpieczeństwa świadczy usługi na rzecz:

1) Kancelarii Prezydenta RP,
2) Kancelarii Sejmu,
3) Kancelarii Senatu,
4) Kancelarii Prezesa Rady Ministrów,
5) Biuru Bezpieczeństwa Narodowego;
6) urzędom obsługującym 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,
7) Siłom Zbrojnym Rzeczypospolitej Polskiej oraz jednostkom organizacyjnym podległym lub nadzorowanym przez Ministra Obrony Narodowej,
8) instytucjom wykonującym 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,

– na wniosek tych podmiotów.

2. Operator strategicznej sieci bezpieczeństwa świadczy usługi:

1) Ministrowi Obrony Narodowej w zakresie:
   a) utrzymania, rozbudowy i modyfikacji sieci teleinformatycznej na potrzeby obsługi Sił Zbrojnych Rzeczypospolitej Polskiej,
   b) zestawienia i utrzymania łączy dostępowych do sieci, o której mowa w lit. a;
2) ministrowi właściwemu do spraw wewnętrznych w zakresie:
   a) utrzymania, rozbudowy i modyfikacji sieci teleinformatycznej na potrzeby obsługi numerów alarmowych,
   b) zestawienia i utrzymania łączy dostępowych do sieci, o której mowa w lit. a, dla:
      – użytkowników centralnej ewidencji pojazdów i centralnej ewidencji kierowców,
      – jednostek Państwowej Straży Pożarnej,
      – dyspozytorni Państwowego Ratownictwa Medycznego i Lotniczego Pogotowia Ratunkowego,
      – Centrum Personalizacji Dokumentów,
      – Zakładu Emerytalno-Rentowego Ministerstwa Spraw Wewnętrznych,
   c) utrzymania i rozbudowy sieci teleinformatycznej na potrzeby rejestru mieszkańców, rejestru zamieszkania cudzoziemców i rejestru stanu cywilnego,
   d) utrzymania i rozbudowy sieci teleinformatycznej GovNet,
   e) utrzymania i rozbudowy sieci teleinformatycznej na potrzeby rejestru PESEL,
   f) zapewnienia połączenia centrów powiadamiania ratunkowego z publiczną siecią telekomunikacyjną;
3) ministrowi właściwemu do spraw zagranicznych w zakresie:
   a) świadczenia usług telekomunikacyjnych w systemie łączności satelitarnej,
   b) świadczenia usług sieci rozległej.

3. Podmioty, o których mowa w ust. 2, obowiązane są korzystać z usług telekomunikacyjnych w ruchomej publicznej sieci telekomunikacyjnej świadczonych przez Operatora strategicznej sieci bezpieczeństwa w zakresie zapewnienia realizacji

zadań w tych podmiotach na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

4. Prezes Rady Ministrów może zobowiązać Operatora strategicznej sieci bezpieczeństwa do świadczenia usług, o których mowa w art. 76c ust. 1:

1) właścicielom i posiadaczom obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, lub
2) przedsiębiorcom, o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców.

5. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne oraz Komenda Główna Policji mogą zlecić Operatorowi strategicznej sieci bezpieczeństwa świadczenie usługi wsparcia technicznego, z uwzględnieniem prac badawczo-rozwojowych dotyczących nowoczesnych systemów łączności.

6. Świadczenie usług, o których mowa w ust. 1 i 2 oraz art. 76c ust. 1, przez Operatora strategicznej sieci bezpieczeństwa wymaga zawarcia umowy pomiędzy Operatorem strategicznej sieci bezpieczeństwa a właściwym podmiotem, o którym mowa w ust. 1 i 2.

7. Umowa, o której mowa w ust. 6, określa w szczególności obowiązek zapewnienia przez Operatora strategicznej sieci bezpieczeństwa usług telekomunikacyjnych o określonej jakości usług, co najmniej w przypadkach zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego.

Art. 76e. Przy zawieraniu umów, o których mowa w art. 76d ust. 6, dotyczących realizacji zadań, o których mowa w art. 76a ust. 1, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 i 1598).

Art. 76f. 1. Prezes UKE, w drodze decyzji, na wniosek Operatora strategicznej sieci bezpieczeństwa, nakłada na operatora, o którym mowa w art. 2 pkt 27 lit. b ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, obowiązek kolokacji oraz udostępniania, w tym współkorzystania z infrastruktury telekomunikacyjnej, która została umieszczona na nieruchomości w związku z wykonywaniem uprawnień wynikających z przepisów prawa, wyroku sądu lub decyzji, na rzecz Operatora strategicznej sieci bezpieczeństwa i w celu

realizacji zadań, o których mowa w art. 76a ust. 1, o ile operator nie wykaże, że jest to technicznie niemożliwe.

2. Dostęp, o którym mowa w ust. 1, jest odpłatny. Opłata za ten dostęp umożliwia zwrot proporcjonalnej części poniesionych kosztów powstania tej infrastruktury oraz ponoszonych kosztów jej utrzymania oraz uwzględnia wpływ zapewnienia tego dostępu na plan biznesowy operatora, w szczególności na realizowane przez niego inwestycje.

Art. 76g. 1. Na potrzeby realizacji zadań, o których mowa w art. 76a ust. 1:

1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa, oraz
2) jednostka samorządu terytorialnego,

– zapewnia Operatorowi strategicznej sieci bezpieczeństwa dostęp do nieruchomości, w tym do budynku, polegający na umożliwieniu umieszczenia na niej infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia jej wartości.

2. Warunki dostępu, o którym mowa w ust. 1, określa odpowiednio umowa zawarta pomiędzy Operatorem strategicznej sieci bezpieczeństwa a podmiotami, o których mowa w ust. 1.

3. Umowa, o której mowa w ust. 2, jest zawierana w formie pisemnej w terminie 30 dni od dnia wystąpienia przez Operatora strategicznej sieci bezpieczeństwa z wnioskiem o jej zawarcie.

4. Dostęp, o którym mowa w ust. 1, jeżeli podmiotem zapewniającym dostęp jest:

1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu jest nieodpłatny;
2) jednostka samorządu terytorialnego, jest nieodpłatny, przy czym Operator strategicznej sieci bezpieczeństwa ponosi:
   a) proporcjonalną część kosztów administracyjnych, poniesionych przy zarządzaniu, sprawowaniu nadzoru lub zarządzaniu tą nieruchomością,
   b) proporcjonalną część kosztów, które wystąpiły po stronie jednostki samorządu terytorialnego, jeżeli są konieczne i zaistniały bezpośrednio na skutek zapewnienia takiego dostępu,
   c) koszty przywrócenia nieruchomości do stanu poprzedniego.

Art. 76h. 1. Do dostępu, o którym mowa w art. 76f ust. 1 oraz art. 76g ust. 1, przepisy art. 26–32 oraz 33 ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stosuje się odpowiednio.

2. Od decyzji Prezesa UKE dotyczącej dostępu telekomunikacyjnego, o którym mowa w art. 76f ust. 1 oraz art. 76g ust. 1, przysługuje odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

Art. 76i. Operatorowi strategicznej sieci bezpieczeństwa przysługuje prawo pierwokupu sieci telekomunikacyjnych będących własnością:

1) Skarbu Państwa lub innych państwowych osób prawnych, w szczególności podmiotów, o którym mowa w art. 4 pkt 1, 2, 4, 5, 7 i 8 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
2) jednostek samorządu terytorialnego.

Art. 76j. W zakresie nieuregulowanym w ustawie do Operatora strategicznej sieci bezpieczeństwa stosuje się przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Art. 76k. 1. W przypadku, w którym podmiot wyznaczony na Operatora strategicznej sieci bezpieczeństwa przestaje spełniać którąkolwiek z przesłanek, o których mowa w art. 76a ust. 3, Prezes Rady Ministrów może, w drodze zarządzenia:

1) odwołać Operatora strategicznej sieci bezpieczeństwa, oraz
2) wyznaczyć nowego Operatora strategicznej sieci bezpieczeństwa.

2. W zarządzeniu, o którym mowa w ust. 1, Prezes Rady Ministrów może wyznaczyć termin odwołania oraz wyznaczenia.

Art. 76l. W przypadku, o którym mowa w art. 76i ust. 1:

1) podmiot wyznaczony na nowego Operatora strategicznej sieci bezpieczeństwa jest następcą prawnym dotychczasowego Operatora strategicznej sieci bezpieczeństwa w zakresie realizacji zadań, o których mowa w art. 76a ust. 1.
2) umowy, o których mowa w art. 76d ust. 6, wygasają z mocy prawa w terminie 3 miesięcy od wydania zarządzenia.

Rozdział 2

Spółka Polskie 5G

Art. 76m. 1. W celu realizacji ogólnopolskiej hurtowej sieci 5G na zakresach częstotliwości, o których mowa w art. 76o ust. 1 i art. 76p ust. 1, Operator strategicznej

sieci bezpieczeństwa tworzy spółkę kapitałową, która będzie pełnić funkcję operatora tej sieci, zwaną dalej: „Spółka Polskie 5G”.

2. Kapitał zakładowy Spółki Polskie 5G wynosi 1 000 000 zł (jeden milion złotych). Kapitał zakładowy może zostać zmieniony decyzją udziałowców albo akcjonariuszy Spółki Polskie 5G.

3. Akt założycielski Spółki Polskie 5G określa w szczególności:

1) zasady podziału udziałów albo akcji Spółki Polskie 5G z uwzględnieniem art. 76n ust. 1;
2) prawa i obowiązki udziałowców albo akcjonariuszy;
3) zasady wykonywania prawa głosu z udziałów lub akcji;
4) kompetencje, zasady powoływania i zasady podejmowania uchwał przez zarząd i radę nadzorczą spółki, oraz kompetencje i zasady podejmowania uchwał przez zgromadzenie udziałowców albo walne zgromadzenie akcjonariuszy;
5) zadania realizowane przez Spółkę Polskie 5G;
6) warunki świadczenia usług hurtowych przez Spółkę Polskie 5G na rzecz udziałowców lub akcjonariuszy, w tym warunki finansowe;
7) zobowiązania udziałowców albo akcjonariuszy do budowy oraz udostępnienia posiadanej infrastruktury telekomunikacyjnej na rzecz Spółki Polskie 5G, do której tytuł prawny posiadają akcjonariusze albo udziałowcy zapewniającej dostęp do sieci we wskazanych obszarach kraju, w szczególności wzdłuż głównych szlaków komunikacyjnych, oraz warunki, na jakich infrastruktura ta będzie udostępniana;
8) zobowiązanie Spółki Polskie 5G do budowy lub zapewnienia infrastruktury telekomunikacyjnej zapewniającej dostęp do sieci we wskazanych obszarach kraju, w tym w szczególności wzdłuż głównych szlaków komunikacyjnych;
9) określa warunki udostępniania przez Spółkę Polskie 5G infrastruktury telekomunikacyjnej oraz świadczenia usług telekomunikacyjnych Operatorowi sieci strategicznej bezpieczeństwa, w tym możliwość zwiększenia wykorzystania sieci poprzez odpowiednie zarządzanie ruchem, w szczególności poprzez jego priorytetyzację, w sytuacjach szczególnego zagrożenia;
10) zasady finansowania spółki, w tym zasady dokapitalizowania spółki przez udziałowców albo akcjonariuszy;
11) politykę dystrybucji środków, w tym wypłaty dywidendy;
12) zasady zbywania udziałów albo akcji.

Art. 76n. 1. Udziały albo akcje 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. 76o ust. 1.

2. Podmioty, o których mowa w ust. 1 pkt 1 i 2, dysponują na zgromadzeniu wspólników albo na walnym zgromadzeniu akcjonariuszy liczbą głosów co najmniej równą liczbie posiadanych udziałów w Spółce Polskie 5G.

3. Rada nadzorcza Spółki Polskie 5G składa się z 5 członków: 3 powoływanych przez podmioty o których mowa w ust. 1 pkt 1 i 2, oraz 2 powoływanych przez podmiot lub podmioty wskazane w ust. 1 pkt 3. Kadencja rady nadzorczej trwa 3 lata.

4. Zarząd Spółki Polskie 5G składa się z 4 członków: 2, w tym prezes zarządu, powoływanych przez podmioty wskazane w ust. 1 pkt 1 i 2, oraz dwóch powoływanych przez podmiot lub podmioty wskazane w ust. 1 pkt 3. Kadencja zarządu trwa 3 lata. Poszczególni członkowie mogą być odwoływani przez oświadczenie uprawnionych udziałowców albo akcjonariuszy. Prezes zarządu ma głos rozstrzygający w przypadku równości głosów.

5. Spółka Polskie 5G w oparciu o częstotliwości, o których mowa w art. 76o ust. 1 oraz 76p ust. 1, udostępnioną przez akcjonariuszy infrastrukturę telekomunikacyjną oraz własną nowo wybudowaną, nabytą lub udostępnianą przez podmioty trzecie infrastrukturę telekomunikacyjną, tworzy ogólnopolską hurtową sieć 5G.

6. Spółka Polskie 5G jest obowiązana do:

1) odpłatnego oferowania usług telekomunikacyjnych na warunkach hurtowych,

2) udostępniania odpłatnie usług telekomunikacyjnych Operatorowi strategicznej sieci bezpieczeństwa do świadczenia przez niego usług, o których mowa w art. 76c ust. 4, oraz
3) zapewnienia pokrycia całego terytorium kraju zasięgiem sieci hurtowej oraz zapewnienia szczególnego poziomu bezpieczeństwa w interesie publicznym w zakresie sieci oraz usług.

Rozdział 3

Przyznanie częstotliwości z zakresu 703 – 733 MHz oraz 758 – 788 MHz

Art. 76o. 1. Prezes UKE, w drodze decyzji, przydziela Operatorowi strategicznej sieci bezpieczeństwa częstotliwości rządowe w zakresie 703-713 MHz oraz 758-768 MHz.

2. Do decyzji, o której mowa w ust. 1, przepisy art. 114 oraz art. 115 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne stosuje się odpowiednio.

3. W decyzji, o której mowa w ust. 1, Prezes UKE określa wymogi pokrycia zasięgiem ruchomych sieci telekomunikacyjnych opartych o częstotliwości, o których mowa w ust. 1.

Art. 76p. 1. Częstotliwości w zakresie 713-733 MHz oraz 768-788 MHz Prezes UKE może przyznać przedsiębiorcy telekomunikacyjnemu lub konsorcjum przedsiębiorców telekomunikacyjnych w drodze przetargu, o którym mowa w art. 116 ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, do świadczenia wyłącznie usług hurtowych.

2. Wśród kryteriów przetargu, o którym mowa w ust. 1, oprócz kryteriów wskazanych w art. 118a ust. 1 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne, jest zapewnienie przy świadczeniu usług odpowiedniego poziomu bezpieczeństwa oraz niezawodności sieci i usług.

3. Prezes UKE, spośród kryteriów, o których mowa w ust. 2 oraz w art. 118a ust. 1 pkt 1 i 2 ustawy Prawo telekomunikacyjne, dokonuje w dokumentacji przetargowej wyboru najistotniejszego kryterium oceny ofert w przetargu, mając na uwadze cele polityki regulacyjnej i stan konkurencji na rynku.

Art. 76r. 1. W rezerwacji częstotliwości w zakresie 713-733 MHz oraz 768-788 MHz Prezes UKE może również określić obowiązek współużytkowania tych częstotliwości

oraz częstotliwości w zakresie 703-713 MHz oraz 758-768 MHz w ramach ogólnopolskiej hurtowej sieci.

2. W decyzji, o której mowa w art. 76o, Prezes UKE może określić obowiązek współużytkowania częstotliwości, o których mowa w art. 76o ust. 1 oraz w art. 76p ust. 1.

3. Częstotliwości, o których mowa w art. 76o ust. 1 oraz w art. 76p ust. 1, mogą być współużytkowane w ramach jednej sieci telekomunikacyjnej.

Art. 76s. 1. W przypadku wydania przez Prezesa Rady Ministrów zarządzenia, o którym mowa w art. 76k ust. 1, nowy Operator strategicznej sieci bezpieczeństwa, obejmuje prawa i obowiązki wynikające z przyznania częstotliwości, o którym mowa w art. 76o ust. 1.

2. Prezes UKE potwierdza, w drodze zaświadczenia, przejęcie przez nowego Operatora strategicznej sieci bezpieczeństwa, praw i obowiązków wynikających z przyznania częstotliwości, o którym mowa w art. 76o ust. 1.

3. Zaświadczenie, o którym mowa w ust. 2, wydaje się na wniosek nowego Operatora strategicznej sieci bezpieczeństwa.

Rozdział 4

Fundusz celowy na rzecz strategicznej sieci bezpieczeństwa

Art. 76t 1. Tworzy się Fundusz celowy na rzecz strategicznej sieci bezpieczeństwa, którego dysponentem jest minister właściwy do spraw aktywów państwowych.

2. Fundusz jest państwowym funduszem celowym.

3. Organ obowiązany do pobrania opłat jednorazowych za rezerwacje częstotliwości w zakresie 713-733 MHz oraz 768-788 MHz oraz 3,4 – 3,8 GHz oraz opłat rocznych za prawo do dysponowania tymi częstotliwością, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne ma obowiązek, w terminie, o którym mowa w przepisach wydanych na podstawie ust. 6, przekazywać 50% należnych opłat na rachunek Funduszu.

4. Przychodami Funduszu są:

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 GHz oraz

3) 50% opłat rocznych za prawo do dysponowania tymi częstotliwościami, o których mowa w ustawie Prawo telekomunikacyjne.

5. Środki Funduszu przeznacza się na finansowanie wydatków związanych z:

1) budową infrastruktury na potrzeby strategicznej sieci bezpieczeństwa;
2) zapewnieniem niezawodności funkcjonalności usług świadczonych przez operatora strategicznej sieci bezpieczeństwa w ruchomej sieci telekomunikacyjnej w zakresie zapewnienia realizacji zadań w tych podmiotach na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji;
3) pracami badawczo-rozwojowymi w zakresie usług świadczonych przez operatora strategicznej sieci bezpieczeństwa w ruchomej sieci telekomunikacyjnej w zakresie zapewnienia realizacji zadań w tych podmiotach na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie telekomunikacji;
4) udostępnieniem usług telekomunikacyjnych przez Spółkę Polskie 5G na rzecz operatora strategicznej sieci bezpieczeństwa w celu świadczenia usług przez operatora strategicznej sieci bezpieczeństwa w oparciu o częstotliwości, o których mowa w art. 76o ust. 1.

6. Rada Ministrów określi w drodze rozporządzenia:

1) tryb i zasady pobierania, ewidencjonowania, przekazywania i rozliczania przychodów Funduszu przez organ zobowiązany do ich pobierania;
2) terminy przekazywania i rozliczania opłat jednorazowych za rezerwacje częstotliwości w zakresie 713-733 MHz oraz 768-788 MHz oraz 3,4–3,8 GHz oraz opłat rocznych za prawo do dysponowania częstotliwością

– mając na względzie przeznaczenie środków funduszu oraz racjonalne gospodarowanie tymi środkami, a także zapewnienie przejrzystości procedur.”.

57) po art. 76 dodaje się oznaczenie i tytuł działu oraz w brzmieniu:

„DZIAŁ IV.

Przepisy końcowe.”;

58) w oznaczeniu rozdziału „15” zastępuje się „1”;
59) w art. 93 uchyla się ust. 8 i ust. 23;
60) w załączniku nr 1 do ustawy:

a) w wierszu „Ochrona zdrowia” w kolumnie trzeciej „Rodzaj podmiotów:

:

– skreśla się wiersz czwarty „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2020 r. poz. 944).”,

– skreśla się wiersz piąty „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.”,

b) w wierszu „Infrastruktura cyfrowa” w kolumnie trzeciej „Rodzaj podmiotów” po wierszu „Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).” dodaje się wiersz w brzmieniu „Operator strategicznej sieci bezpieczeństwa”;

61) po załączniku nr 2 do ustawy dodaje się załącznik nr 3 w brzmieniu określonym w załączniku do niniejszej ustawy.

Art. 2. W ustawie z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2021 r. poz. 1486 i 1728) wprowadza się następujące zmiany:

1) w art. 112 po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Funkcjonariuszowi, realizującemu zadania, o których mowa w art. 62a ust. 1 pkt 5 lit. f ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), poza świadczeniami pieniężnymi, o których mowa w ust. 1, przysługuje dodatek, o którym mowa w art. 62a tej ustawy. Dodatek jest wypłacany jako świadczenie teleinformatyczne.”;

2) po art. 115 dodaje się art. 115a w brzmieniu:

„Art. 115a. 1. Do ustalenia wysokości świadczenia teleinformatycznego, o którym mowa w art. 112 ust. 1a, stosuje się przepisy wydane na podstawie art. 62a ust. 10 ustawy o krajowym systemie cyberbezpieczeństwa.

2. Świadczenie teleinformatyczne jest przyznawane na czas wykonywania zadań, o których mowa w art. 112 ust. 1a.

3. Przyznania i cofnięcia świadczenia teleinformatycznego dokonuje kierownik komórki organizacyjnej Komendy Głównej Straży Granicznej, Komendant BSWSG, komendant oddziału Straży Granicznej, komendant ośrodka szkolenia Straży Granicznej, komendant ośrodka Straży Granicznej przyznają w formie rozkazu personalnego będącego decyzją administracyjną.

4. Świadczenia teleinformatycznego nie przyznaje się funkcjonariuszowi:

1) przeciwko któremu wszczęto postępowanie karne o przestępstwo ścigane z oskarżenia publicznego lub postępowanie dyscyplinarne do czasu prawomocnego zakończenia tego postępowania;
2) ukaranemu karą dyscyplinarną - do czasu jej zatarcia;
3) tymczasowo aresztowanemu;
4) skazanemu wyrokiem sądu za przestępstwo ścigane z oskarżenia publicznego

lub w stosunku do którego postępowanie karne o przestępstwo ścigane z oskarżenia publicznego zostało warunkowo umorzone – przez okres jednego roku od dnia uprawomocnienia się orzeczenia.

5. Jeżeli po przyznaniu świadczenia teleinformatycznego funkcjonariusz przestanie realizować zadania, o których mowa w ust. 1 albo wystąpią okoliczności, o których mowa w ust. 4, kierownik komórki organizacyjnej Komendy Głównej Straży Granicznej, Komendant BSWSG, komendant oddziału Straży Granicznej, komendant ośrodka szkolenia Straży Granicznej, komendant ośrodka Straży Granicznej niezwłocznie wydaje rozkaz personalny będący decyzją administracyjną w przedmiocie cofnięcia świadczenia teleinformatycznego.

6. Świadczenia teleinformatycznego nie wypłaca się za okres:
1) korzystania z urlopu bezpłatnego;
2) przerw w wykonywaniu obowiązków służbowych, wymienionych w art. 130 ust. 1-3, za które funkcjonariusz nie zachował prawa do uposażenia;
3) zawieszenia w czynnościach służbowych;
4) zwolnienia od zajęć służbowych, o którym mowa w art. 125b ust. 2 pkt 1 i 3-5;
5) innej nieobecności trwającej co najmniej jeden miesiąc, z wyłączeniem urlopu wypoczynkowego lub dodatkowego, o którym mowa w art. 87b ust. 4, proporcjonalnie do tego okresu.

7. Jeżeli funkcjonariusz pobrał już świadczenie teleinformatyczne za czas nieobecności, o których mowa w ust. 6, potrąca mu się za każdy dzień 1/30 część świadczenia teleinformatycznego przy najbliższej wypłacie uposażenia lub z należności przysługujących mu z tytułu zwolnienia ze służby albo funkcjonariusz zwraca odpowiednią część świadczenia teleinformatycznego w dniu ustania stosunku służbowego.

8. Świadczenie teleinformatyczne płatne jest w terminie płatności uposażenia.

9. Prawo do świadczenia teleinformatycznego wygasa z ostatnim dniem miesiąca, w którym rozkaz personalny, o którym mowa w ust. 5, stał się wykonalny lub nastąpiło rozwiązanie stosunku służbowego w związku ze zwolnieniem funkcjonariusza ze służby albo nastąpiło wygaśnięcie stosunku służbowego w związku ze śmiercią funkcjonariusza.”.

Art. 3. W ustawie z dnia 10 grudnia 1993 r. o zaopatrzeniu emerytalnym żołnierzy zawodowych oraz ich rodzin (Dz. U. z 2020 r. poz. 586 i 2320) wprowadza się następujące zmiany:

1) w art. 5 po ust. 1 dodaje się ust. 1a. w brzmieniu:

„1a. Świadczenia teleinformatycznego, o którym mowa w art. 80a ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz. U. z 2021 r. poz. 1131 i 1666), nie wlicza się do podstawy wymiaru emerytury lub renty inwalidzkiej, o której mowa w ust. 1.”;

2) w art. 6a po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Świadczenia teleinformatycznego, o którym mowa w art. 80a ustawy z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych, nie wlicza się do uposażenia stanowiącego podstawę wymiaru składek na ubezpieczenie emerytalne i rentowe, o którym mowa w ust. 2.”.

Art. 4. W ustawie z dnia 18 lutego 1994 r. o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Straży Marszałkowskiej, Służby Ochrony Państwa, Państwowej Straży Pożarnej, Służby Celno-Skarbowej i Służby Więziennej oraz ich rodzin (Dz. U. 2020 r. poz. 723 i 2320) w art. 5 po ust. 1a dodaje się ust. 1b w brzmieniu:

„1b. Świadczenia teleinformatycznego, o którym mowa w art. 62a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), nie wlicza się do podstawy wymiaru emerytury lub renty inwalidzkiej, o której mowa w ust. 1.”.

Art. 5. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2020 r. poz. 27 i 2320) wprowadza się następujące zmiany:

1) w art. 123 po ust. 1 dodaje się ust. la w brzmieniu:

„1a. Funkcjonariuszowi, realizującemu zadania, o których mowa w art. 62a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), poza świadczeniami pieniężnymi, o których mowa w ust. 1, przysługuje dodatek, o którym mowa w art. 62a ust. 1 tej ustawy. Dodatek jest wypłacany jako świadczenie teleinformatyczne. ”;

2) po art. 126 dodaje się art. 126a w brzmieniu:

„Art. 126a. 1. Do ustalenia wysokości świadczenia teleinformatycznego, o którym mowa w art. 123 ust. 1a, stosuje się przepisy wydane na podstawie art. 62a ust. 12 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369).

2. Świadczenie teleinformatyczne jest przyznawane na czas wykonywania zadań, o których mowa w art. 123 ust. 1a.

3. Przyznania i cofnięcia świadczenia teleinformatycznego dokonuje Szef ABW w formie rozkazu personalnego będącego decyzją administracyjną.

4. Świadczenia teleinformatycznego nie przyznaje się funkcjonariuszowi:

1) przeciwko któremu wszczęto postępowanie karne lub dyscyplinarne do czasu prawomocnego zakończenia tego postępowania;
2) ukaranemu karą dyscyplinarną – do czasu jej zatarcia;
3) tymczasowo aresztowanemu;
4) skazanemu wyrokiem sądu lub w stosunku do którego postępowanie karne zostało warunkowo umorzone – przez okres jednego roku od dnia uprawomocnienia się orzeczenia.

5. Jeżeli po przyznaniu świadczenia teleinformatycznego funkcjonariusz przestanie realizować zadania, o których mowa w ust. 1 albo wystąpią okoliczności, o których mowa w ust. 4, Szef ABW niezwłocznie wydaje rozkaz personalny będący decyzją administracyjną w przedmiocie cofnięcia świadczenia teleinformatycznego.

6. Świadczenia teleinformatycznego nie wypłaca się za okres:

1) korzystania z urlopu bezpłatnego,
2) przerw w wykonywaniu obowiązków służbowych, wymienionych w art. 141 ust. 1-3, za które funkcjonariusz ABW nie zachował prawa do uposażenia,
3) zawieszenia w czynnościach służbowych,
4) zwolnienia od zajęć służbowych, o którym mowa w art. 136b ust. 2 pkt 1 i 3-5,

5) innej nieobecności trwającej co najmniej jeden miesiąc, z wyłączeniem urlopu wypoczynkowego lub dodatkowego, o którym mowa w art. 97 ust. 1 i 2, proporcjonalnie do tego okresu.

7. Jeżeli funkcjonariusz pobrał już świadczenie teleinformatyczne za czas nieobecności, o których mowa w ust. 6, potrąca mu się za każdy dzień 1/30 część świadczenia teleinformatycznego przy najbliższej wypłacie uposażenia lub z należności przysługujących mu z tytułu zwolnienia ze służby albo funkcjonariusz zwraca odpowiednią część świadczenia teleinformatycznego w dniu ustania stosunku służbowego.

8. Świadczenie teleinformatyczne wypłaca się w każdym kolejnym miesiącu kalendarzowym, począwszy od miesiąca następującego po miesiącu, w którym został wydany rozkaz personalny będący decyzją administracyjną o przyznaniu świadczenia teleinformatycznego.

9. Świadczenie teleinformatyczne płatne jest w terminie płatności uposażenia.

10. Prawo do świadczenia teleinformatycznego wygasa z ostatnim dniem miesiąca, w którym rozkaz personalny, o którym mowa w ust. 5, stał się wykonalny lub nastąpiło rozwiązanie stosunku służbowego w związku ze zwolnieniem funkcjonariusza ABW ze służby albo nastąpiło wygaśnięcie stosunku służbowego w związku ze śmiercią funkcjonariusza ABW.

Art. 6. W ustawie z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych (Dz. U. z 2021 r. poz. 1131 i 1666), po art. 80 dodaje się art. 80a w brzmieniu:

„80a. 1. Żołnierzowi zawodowemu, realizującemu zadania, o których mowa w art. 62a ust. 1 pkt 1 i 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), poza świadczeniami pieniężnymi, o których mowa w ust. 1, przysługuje dodatek, o którym mowa w art. 62a tej ustawy. Dodatek jest wypłacany jako świadczenie teleinformatyczne.

2. Do ustalenia wysokości świadczenia teleinformatycznego, o którym mowa w ust. 1, stosuje się przepisy wydane na podstawie art. 62a ust. 12 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

3. Świadczenie teleinformatyczne jest przyznawane na czas wykonywania zadań, o których mowa w ust. 1.

4. Przyznania i cofnięcia świadczenia teleinformatycznego dokonuje organ, o którym mowa w art. 104, w formie rozkazu personalnego będącego decyzją administracyjną.

5. Świadczenia teleinformatycznego nie przyznaje się żołnierzowi zawodowemu:

1) przeciwko któremu wszczęto postępowanie karne o przestępstwo ścigane z oskarżenia publicznego lub postępowanie dyscyplinarne do czasu prawomocnego zakończenia tego postępowania;
2) ukaranemu karą dyscyplinarną – do czasu jej zatarcia;
3) tymczasowo aresztowanemu;
4) skazanemu wyrokiem sądu za przestępstwo ścigane z oskarżenia publicznego

lub w stosunku do którego postępowanie karne o przestępstwo ścigane z oskarżenia publicznego zostało warunkowo umorzone – przez okres jednego roku od dnia uprawomocnienia się orzeczenia.

6. Jeżeli po przyznaniu świadczenia teleinformatycznego żołnierz zawodowy przestanie realizować zadania, o których mowa w ust. 1 albo wystąpią okoliczności, o których mowa w ust. 4, organ, który przyznał świadczenie, niezwłocznie wydaje rozkaz personalny będący decyzją administracyjną w przedmiocie cofnięcia świadczenia teleinformatycznego.

7. Świadczenia teleinformatycznego nie wypłaca się za okres:

1) korzystania z urlopu bezpłatnego;
2) przerw w wykonywaniu obowiązków służbowych, wymienionych w art. 93, za które funkcjonariusz nie zachował prawa do uposażenia;
3) zawieszenia w czynnościach służbowych;
4) zwolnienia od zajęć służbowych, o którym mowa w art. 60b ust. 1 pkt 1 i 3-6.
5) innej nieobecności trwającej co najmniej jeden miesiąc, z wyłączeniem urlopu wypoczynkowego lub dodatkowego, o którym mowa w art. 62 ust. 2, proporcjonalnie do tego okresu.

8. Jeżeli funkcjonariusz pobrał już świadczenie teleinformatyczne za czas nieobecności, o których mowa w ust. 7, potrąca mu się za każdy dzień 1/30 część świadczenia teleinformatycznego przy najbliższej wypłacie uposażenia lub z należności przysługujących mu z tytułu zwolnienia ze służby albo funkcjonariusz zwraca odpowiednią część świadczenia teleinformatycznego w dniu ustania stosunku służbowego.

9. Świadczenie teleinformatyczne płatne jest w terminie płatności uposażenia.

10. Prawo do świadczenia teleinformatycznego wygasa z ostatnim dniem miesiąca, w którym rozkaz personalny, o którym mowa w ust. 6, stał się wykonalny lub nastąpiło rozwiązanie stosunku służbowego w związku ze zwolnieniem żołnierza zawodowego ze służby albo nastąpiło wygaśnięcie stosunku służbowego w związku ze śmiercią funkcjonariusza.”.

Art. 7. W ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2021 r. poz. 1671) wprowadza się następując zmiany:

1) w art. 92 po ust. 1 dodaje się ust. la w brzmieniu:

„1a. Funkcjonariuszowi, realizującemu zadania, o których mowa w art. 62a ust. 1 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369), poza świadczeniami pieniężnymi, o których mowa w ust. 1, przysługuje świadczenie teleinformatyczne wypłacane jako dodatek.”;

2) po art. 99 dodaje się art. 99a w brzmieniu:

„Art. 99a. 1. Do świadczenia teleinformatycznego, o którym mowa w art. 123 ust. 1a, stosuje się art. 62a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, z zastrzeżeniem przepisów niniejszej ustawy.

2. Świadczenie teleinformatyczne jest przyznawane na czas wykonywania zadań, o których mowa w art. 92 ust. 1a.

3. Szef CBA przyznaje i cofa świadczenia teleinformatycznego w drodze decyzji.

4. Świadczenia teleinformatycznego nie przyznaje się funkcjonariuszowi:

1) przeciwko któremu wszczęto postępowanie karne lub dyscyplinarne do czasu prawomocnego zakończenia tego postępowania;
2) ukaranemu karą dyscyplinarną - do czasu jej zatarcia;
3) tymczasowo aresztowanemu;
4) skazanemu wyrokiem sądu lub w stosunku do którego postępowanie karne zostało warunkowo umorzone - przez okres jednego roku od dnia uprawomocnienia się orzeczenia.

5. Jeżeli po przyznaniu świadczenia teleinformatycznego funkcjonariusz przestanie realizować zadania, o których mowa w ust. 1a albo wystąpią okoliczności, o których mowa w ust. 4, Szef CBA niezwłocznie cofa decyzję o przyznaniu świadczenia teleinformatycznego.

6. Świadczenia teleinformatycznego nie wypłaca się za okres:

1) korzystania z urlopu bezpłatnego,
2) przerw w wykonywaniu obowiązków służbowych, wymienionych w art. 105 ust. 1-3, za które funkcjonariusz nie zachował prawa do uposażenia,
3) zawieszenia w czynnościach służbowych,
4) zwolnienia od zajęć służbowych, o którym mowa w art. 102b ust. 2 pkt 1 i 3-5,
5) innej nieobecności trwającej co najmniej jeden miesiąc, z wyłączeniem urlopu wypoczynkowego lub dodatkowego, o którym mowa w art. 85 ust. 1, proporcjonalnie do tego okresu.

7. Świadczenie teleinformatyczne wypłaca się w każdym kolejnym miesiącu kalendarzowym, począwszy od miesiąca następującego po miesiącu, w którym została wydana decyzja o przyznaniu świadczenia teleinformatycznego.

8. Świadczenie teleinformatyczne płatne jest w terminie płatności uposażenia.

9. Prawo do świadczenia teleinformatycznego wygasa z ostatnim dniem miesiąca, w którym decyzja, o której mowa w ust. 5, stała się wykonalna lub nastąpiło rozwiązanie stosunku służbowego w związku ze zwolnieniem funkcjonariusza ze służby albo nastąpiło wygaśnięcie stosunku służbowego w związku ze śmiercią funkcjonariusza.”.

Art. 8. W ustawie z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz. U. z 2021 r. poz. 1362) wprowadza się następujące zmiany:

1) po art. 15 dodaje się art. 15a w brzmieniu:

„Art. 15a. 1. Funkcjonariuszowi można powierzyć wykonywanie obowiązków, o których mowa w art. 62a ust. 1 pkt 1 i 5 lit. d-e ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369) (obowiązki eksperta). Przepisu art. 15 ust. 1 zdanie pierwsze nie stosuje się.

2. Obowiązki eksperta powierza funkcjonariuszowi Minister Obrony Narodowej, na pisemny wniosek Szefa SKW, Szefa SWW lub kierownika jednostki odpowiedzialnej za zapewnienie prawidłowego funkcjonowania CSIRT MON.

3. Wniosek, o którym mowa w ust. 2, zawiera:

1) dane funkcjonariusza, któremu zamierza się powierzyć wykonywanie obowiązków eksperta;
2) informację o spełnieniu przez funkcjonariusza wymogów określonych w przepisach wydanych na podstawie art. 62a ust. 12 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

3) okres powierzenia wykonywania obowiązków eksperta funkcjonariuszowi;
4) jednostkę organizacyjną, na rzecz której funkcjonariusz będzie wykonywał obowiązki eksperta;
5) zakres zadań, jakie będą wykonywane przez funkcjonariusza w ramach obowiązków eksperta;
6) wysokość proponowanego dla funkcjonariusza świadczenia teleinformatycznego, uwzględniając art. 62a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

4. Powierzając funkcjonariuszowi wykonywanie obowiązków eksperta określa się:
1) jednostkę organizacyjną, na rzecz której funkcjonariusz będzie wykonywał obowiązki eksperta;
2) zakres zadań, jakie będą wykonywane przez funkcjonariusza w ramach obowiązków eksperta;
3) okres, na który funkcjonariuszowi zostają powierzone obowiązki eksperta;
4) wysokość świadczenia teleinformatycznego dla funkcjonariusza.

5. Funkcjonariusz realizuje obowiązki eksperta odpowiednio w SKW lub SWW.

6. Minister Obrony Narodowej może w każdym czasie, z własnej inicjatywy lub na wniosek Szefa SKW albo Szefa SWW albo kierownika jednostki odpowiedzialnej za zapewnienie prawidłowego funkcjonowania CSIRT MON, cofnąć powierzenie obowiązków eksperta.”;

2) w art. 83 w ust. 1 po pkt 4 dodaje się pkt 4a w brzmieniu:
„4a) świadczenie teleinformatyczne, o którym mowa w art. 62b ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;”;

3) po art. 83 dodaje się art. 83a w brzmieniu:

„Art. 83a. 1. Funkcjonariuszowi, o którym mowa w art. 15a, przysługuje świadczenie teleinformatyczne na czas wykonywania obowiązków eksperta w wysokości określonej zgodnie z przepisami wydanymi na podstawie art. 62a ust. 12 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

2. Świadczenie eksperckie nie stanowi dodatku do uposażenia, o którym mowa w art. 79 i nie wlicza się go do:
1) uposażenia stanowiącego podstawę wymiaru składek na ubezpieczenia emerytalne i rentowe, o którym mowa w art. 52 ust. 2;
2) uposażenia otrzymanego w roku kalendarzowym, o którym mowa w art. 85 ust. 1a.

3. Świadczenie teleinformatyczne jest przyznawane na czas określony, jednorazowo na okres nie dłuższy niż 12 miesięcy.

4. Przyznania i cofnięcia świadczenia teleinformatycznego dokonuje Minister Obrony Narodowej w drodze decyzji administracyjnej.

5. Przy ustalaniu wysokości świadczenia teleinformatycznego uwzględnia się w szczególności kwalifikacje zawodowe posiadane przez funkcjonariusza oraz stopień złożoności zadań, o których mowa w art. 62a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

6. Świadczenia teleinformatycznego nie przyznaje się funkcjonariuszowi:

1) przeciwko któremu wszczęto postępowanie karne lub dyscyplinarne do czasu prawomocnego zakończenia tego postępowania;
2) ukaranemu karą dyscyplinarną – do czasu jej zatarcia;
3) tymczasowo aresztowanemu;
4) skazanemu prawomocnym wyrokiem sądu za ścigane z oskarżenia publicznego przestępstwo umyślne lub w stosunku do którego postępowanie karne zostało warunkowo umorzone –do czasu zatarcia odpowiednio skazania lub warunkowego umorzenia postępowania.

7. Jeżeli po przyznaniu świadczenia teleinformatycznego funkcjonariusz przestanie realizować zadania, o których mowa w art. 62a ust. 1 pkt 1 i 5 lit. d-e ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, albo wystąpią okoliczności, o których mowa w ust. 6, Minister Obrony Narodowej niezwłocznie cofa świadczenie.

8. Świadczenie teleinformatyczne wypłaca się miesięcznie, w terminie płatności uposażenia, począwszy od miesiąca następującego po miesiącu, w którym świadczenie eksperckie zostało przyznane.

9. Wysokość świadczenia teleinformatycznego za dany miesiąc obniża się o 1/30 część świadczenia teleinformatycznego za każdy dzień niewykonywania przez funkcjonariusza obowiązków eksperta z powodu:

1) korzystania z urlopu bezpłatnego;
2) przebywania na zwolnieniu lekarskim;
3) przerw w wykonywaniu obowiązków służbowych, wymienionych w art. 101 ust. 1-3, za które funkcjonariusz nie zachował prawa do uposażenia;
4) zawieszenia w czynnościach służbowych;
5) zwolnienia od zajęć służbowych, o którym mowa w art. 96b ust. 2 pkt 1 i 3-5;

6) zaistnienia innych, niż wymienione w pkt 1-5, okoliczności powodujących niewykonywanie przez funkcjonariusza obowiązków eksperta.

10. Prawo do świadczenia teleinformatycznego wygasa z ostatnim dniem miesiąca, w którym nastąpiło zwolnienie funkcjonariusza ze służby lub zaistniały okoliczności uzasadniające wygaśnięcie tego prawa.”;

4) art. 103 otrzymuje brzmienie:

„Art. 103. Przepisu art. 102 ust. 1 i 2 nie stosuje się do świadczenia teleinformatycznego oraz zaliczek pobieranych do rozliczenia, a w szczególności na koszty podróży służbowej, delegacji i przeniesienia. Należności te potrąca się z uposażenia w pełnej wysokości, niezależnie od potrąceń z innych tytułów.”.

Art. 9. W ustawie z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2021 r. poz. 777 i 784) w art. 16a w ust. 3 pkt 1 otrzymuje brzmienie:

„1) 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;”.

Art. 10. W ustawie z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz.U. z 2020 r. poz. 735 oraz z 2021 r. poz. 159, 255, 1551 i 1561) w art. 13 w ust. 1 w pkt 30 kropkę zastępuje się średnikiem i dodaje się pkt 31 w brzmieniu:

„31) podmiot wyznaczony na operatora strategicznej sieci bezpieczeństwa, o którym mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”.

Art. 11. 1. Operatorzy usług kluczowych zgłaszają incydenty poważne za pomocą systemu teleinformatycznego od 1 stycznia 2023 r.

2. Operator usługi kluczowej, któremu została doręczona decyzja o uznaniu za operatora usługi kluczowej po dniu 1 lipca 2022 r., w terminie 6 miesięcy rozpoczyna korzystanie z systemu, o którym mowa w art. 46 ustawy zmienianej w art. 1.

Art. 12. Do postępowań o udzielenie zamówienia publicznego, wszczętych przed dniem wejścia w życie niniejszej ustawy, które, przed dniem opublikowania informacji, o której mowa w art. 66a ust. 1 ustawy zmienianej w art. 1, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, nie zakończyły się wyborem wykonawcy albo unieważnieniem postępowania, stosuje się przepisy ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 13. 1. Tworzy się Fundusz Cyberbezpieczeństwa.

2. W terminie 14 dni od dnia wejścia w życie niniejszego przepisu minister właściwy do spraw informatyzacji przekaże na rachunek Funduszu środki w wysokości do 100.000.000 zł ze środków Funduszu Szerokopasmowego, o którym mowa w art. 16a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2021 r. poz. 777 i 784).

3. W terminie 14 dni od dnia wejścia w życie niniejszego przepisu, minister właściwy do spraw informatyzacji przekaże środki w wysokości do 150.000.000 zł na rachunek Funduszu, ze środków budżetu państwa, z części której jest dysponentem.

4. Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego może przekazać, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji, do dnia 31 grudnia 2022 r. na rachunek Funduszu łącznie środki w wysokości do 100.000.000 zł ze środków z zysku instytutu, w tym z funduszu rezerwowego, o którym mowa w art. 19 ust. 1 pkt 2 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2020 r. poz. 1383 oraz z 2021 r. poz. 1192).

5. Przekazanie środków, o których mowa w ust. 4, ujmuje się w planie finansowym Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, jako odrębną pozycję.

Art. 14. 1. Do czasu wydania komunikatu o osiągnięciu zdolności operacyjnej przez właściwy CSIRT sektorowy operatorzy usług kluczowych zgłaszają incydenty poważne do właściwego CSIRT GOV, CSIRT MON lub CSIRT NASK.

2. Agencja Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym do czasu otrzymania informacji o osiągnięciu zdolności operacyjnej przez CSIRT INT, zgłaszają incydenty w podmiocie publicznym do CSIRT GOV.

Art. 15. 1. Narzędzie do uwierzytelnienia dwuskładnikowego zakupione w ramach realizacji przez NASK-PIB zadania, o którym mowa w art. 37 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, z chwilą przekazania staje się własnością osoby, która je otrzymała.

2. Określone w ust. 1 nabycie narzędzia do uwierzytelnienia dwuskładnikowego nie rodzi zobowiązań podatkowych.

Art. 16. 1. Z dniem wejścia w życie ustawy:

1) wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo powołane w ramach operatora usługi kluczowej przed wejściem w życie niniejszej ustawy stają się SOC powołanymi w ramach operatora usługi kluczowej;
2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się podmiotami prowadzącymi SOC na rzecz operatora usługi kluczowej;
3) sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy w brzmieniu dotychczasowym staje się CSIRT sektorowym.

2. Podmioty publiczne oraz podmiot, o którym mowa w art. 7 ust. 1 pkt 7 ustawy – Prawo o szkolnictwie wyższym, wyznaczają osoby, o których mowa w art. 21 ustawy zmienianej w art. 1 w terminie 30 dni od dnia wejścia w życie niniejszej ustawy.

3. Organ właściwy ustanawia CSIRT sektorowy w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

4. Organ właściwy do spraw cyberbezpieczeństwa publikuje komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w Dzienniku Urzędowym Monitor Polski.

5. Szef Agencji Wywiadu informuje jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym o osiągnięciu przez CSIRT INT zdolności operacyjnej.

6. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT sektorowy jest również publikowana na stronach internetowych:

1) urzędu obsługującego Pełnomocnika,
2) zespołów CSIRT GOV, CSIRT MON, CSIRT NASK,

– a także jest przekazywana za pomocą systemu informacyjnego, o którym mowa w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa.

7. Operator usługi kluczowej realizuje obowiązki, o których mowa w art. 11 ust. 3 pkt 1-3 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą od dnia następującego po

dniu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej.

8. Operator usługi kluczowej wykonuje po raz pierwszy obowiązek, o którym mowa w art. 9 ust. 2 ustawy zmienianej w art. 1, w terminie 14 dni od dnia wejścia w życie niniejszej ustawy.

9. CSIRT GOV, CSIRT MON lub CSIRT NASK dostosowują w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy porozumienia, o których mowa w art. 26 ust. 10 ustawy zmienianej w art. 1, do przepisów ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 17. Z dniem … art. 72a ust. 1 pkt 3 ustawy zmienianej w art. 1 otrzymuje następujące brzmienie:

„3) 50% wpływów z opłat za prawo do wykorzystywania zasobów numeracji, o których mowa w art. 25 ust. 1 ustawy z dnia ... – Prawo komunikacji elektronicznej”;

Art. 18. 1. Prezes Rady Ministrów wyznacza Operatora strategicznej sieci bezpieczeństwa w terminie do 30 dni od wejścia w życie ustawy.

2. Operator strategicznej sieci bezpieczeństwa jest obowiązany powołać Spółkę Polskie 5G w terminie do 60 dni od dnia wyznaczenia Operatora strategicznej sieci bezpieczeństwa, o którym mowa w ust. 1.

3. Akt założycielski Spółki Polskie 5G nie może zostać zmieniony od ogłoszenia przetargu, o którym mowa w art. 76p ust. 1, do czasu objęcia akcji lub udziałów, o których mowa w art. 15 ust. 1 pkt 3. Operator strategicznej sieci bezpieczeństwa udostępni akt założycielski Spółki Polskie 5G w terminie 3 dni roboczych od dnia złożenia wniosku przez podmiot zainteresowany, który wykaże, że wniósł opłatę za dokumentację przetargową dotyczącą przetargu, o którym mowa w art. 76p ust. 1.

Art. 19. Z dniem … w art. 76o ust. 1–2 otrzymują brzmienie:

„1. Prezes UKE, przydziela w drodze przydziału, o którym mowa w art. 72 ust. 1 ustawy Prawo komunikacji elektronicznej, Operatorowi strategicznej sieci bezpieczeństwa częstotliwości rządowe z zakresu 703-713 MHz oraz 758-768 MHz. Przepisy art. 73-79 ustawy Prawo komunikacji elektronicznej stosuje się odpowiednio.

2. Do decyzji, o której mowa w ust. 1, przepisy art. 68, art 69 ust. 1, art. 80, art. 82, art. 84, art. 85 oraz art. 89 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.

Art. 20. Z dniem … art. 17 otrzymuje brzmienie:

„Art. 76p 1. Częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz Prezes UKE może przydzielić przedsiębiorcy telekomunikacyjnemu lub konsorcjum przedsiębiorców telekomunikacyjnych w drodze przetargu, o którym mowa w art. 104 ust. 3 ustawy Prawo komunikacji elektronicznej, do świadczenia wyłącznie usług hurtowych.

2. Wśród kryteriów przetargu, o którym mowa w ust. 1, oprócz kryteriów wskazanych w art. 117 ust. 1 ustawy Prawo komunikacji elektronicznej jest zapewnienie przy świadczeniu usług odpowiedniego poziomu bezpieczeństwa oraz niezawodności sieci i usług.

3. Prezes UKE, spośród kryteriów, o których mowa w ust. 2 oraz w art. 117 ust. 1 pkt 1 i 2 ustawy Prawo komunikacji elektronicznej, dokonuje w dokumentacji przetargowej wyboru najistotniejszego kryterium oceny ofert w przetargu, mając na uwadze cele polityki regulacyjnej i stan konkurencji na rynku.”.

Art. 21. Z dniem … w art. 76c ust. 2 i 3 otrzymują brzmienie:

„2. Operator strategicznej sieci bezpieczeństwa może świadczyć usługi telekomunikacyjne także w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym w rozumieniu art. 62 ust. 2 pkt 2 i 3 ustawy z dnia … Prawo komunikacji elektronicznej. Wykorzystanie częstotliwości użytkowanych jako rządowe przez Operatora strategicznej sieci bezpieczeństwa koordynuje Minister Obrony Narodowej, z wyjątkiem ust. 3.

3. Wykorzystanie częstotliwości, o których mowa w art. 76o ust. 1, przez Operatora strategicznej sieci bezpieczeństwa koordynuje Prezes UKE. Przepisy art. 138 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.”.

Art. 22. Z dniem … w art. 9 ust. 1 otrzymuje brzmienie:

„1. Do dostępu, o którym mowa w art. 76f ust. 1 oraz art. 76g ust. 1, stosuje się przepisy art. 169 ust. 1 i 2, art. 170-172, art. 176 ustawy z dnia ... – Prawo komunikacji elektronicznej z zastrzeżeniem, że umowa o tym dostępie jest przekazywana przez Operatora bezpiecznej sieci strategicznej, oraz odpowiednio przepisy działu III rozdziału 3 ustawy z dnia … 2021 r. – Prawo komunikacji elektronicznej.”

Art. 23. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2021 r. – 0,00 mln zł;

2) w 2022 r. – 20,363 mln zł;
3) w 2023 r. – 41,695 mln zł;
4) w 2024 r. – 56,782 mln zł;
5) w 2025 r. – 52,929 mln zł;
6) w 2026 r. – 51,984 mln zł;
7) w 2027 r. – 55,87 mln zł;
8) w 2028 r. – 59,592 mln zł;
9) w 2029 r. – 69,239 mln zł;
10) w 2030 r. – 69,227 mln zł.

2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 59 – Agencja Wywiadu, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2021 r. – 0 mln zł;
2) w 2022 r. – 6,966 mln zł;
3) w 2023 r. – 5,905 mln zł;
4) w 2024 r. – 6,242 mln zł;
5) w 2025 r. – 6,418 mln zł;
6) w 2026 r. – 6,605 mln zł;
7) w 2027 r. – 6,798 mln zł;
8) w 2028 r. – 6,996 mln zł;
9) w 2029 r. – 7,2 mln zł;
10) w 2030 r. – 7,41 mln zł.

3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 83 – Rezerwy celowe, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2021 r. – 0 mln zł;
2) w 2022 r. – 44,164 mln zł;
3) w 2023 r. – 39,083 mln zł;
4) w 2024 r. – 41,382 mln zł;
5) w 2025 r. – 42,548 mln zł;
6) w 2026 r. – 43,785 mln zł;
7) w 2027 r. – 45,058 mln zł;
8) w 2028 r. – 46,37 mln zł;
9) w 2029 r. – 47,72 mln zł;
10) w 2030 r. – 49,11 mln zł.

4. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętych na dany rok budżetowy maksymalnych limitów wydatków, o których mowa w ust. 1, zostaną zastosowane mechanizmy korygujące polegające na:

1) ograniczeniu finansowania działalności wyznaczonego CSIRT sektorowego wskazanego przez ministra właściwego do spraw informatyzacji;
2) ograniczeniu finansowania działalności CSIRT INT.

5. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1 i 3, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 4 pkt 1, dokonuje minister właściwy do spraw informatyzacji.

6. Szef Agencji Wywiadu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 4 pkt 2, dokonuje Szef Agencji Wywiadu w uzgodnieniu ministrem - członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych.

Art. 24. 1. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą.

2. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 25. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Załącznik do ustawy z dnia …
Załącznik nr 3

KATEGORIE FUNKCJI KRYTYCZNYCH
DLA BEZPIECZEŃSTWA SIECI I USŁUG

1. Uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu.

2. Przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi.

3. Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych.

4. Routing ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm.

5. Zarządzanie połączeniami ze sprzętem użytkownika i sesjami.

6. Wdrażanie, zarządzanie i monitorowanie polityk dostępu do sieci.

7. Przydzielanie elementu sieci dla połączeń z urządzeniami użytkowników.

8. Rejestrowanie, autoryzacja i utrzymanie ciągłości usług sieciowych.

9. Zabezpieczenia sieci przed oddziaływaniem aplikacji zewnętrznych.

10. Zabezpieczenia połączeń z innymi sieciami.