Odwrócona tabela zgodności

Projekt ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw (UC47)

Jedn. red.	Treść przepisu projektu	Uzasadnienie wprowadzenia przepisu
Art. 1 pkt 3 lit. h	po pkt 11 kropkę zastępuje się średnikiem i dodaje się pkt (…) w brzmieniu: „12) ryzyku – należy przez to rozumieć prawdopodobieństwo wystąpienia zagrożenia wraz z jego skutkami, z uwzględnieniem odporności środowiska w którym zagrożenie występuje; 13) zarządzaniu ryzykiem – należy przez to rozumieć działania polegające na: a) planowaniu działań ograniczających ryzyko, b) wdrażaniu działań ograniczających ryzyko, c) osiąganiu gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej, d) okresowej ocenie osiągniętych efektów; 14) ocenie ryzyka - należy przez to rozumieć proces identyfikacji prawdopodobieństwa wystąpienia zagrożenia, podatności na zagrożenie oraz szacowania jego skutków. Wynikiem oceny jest wartość ryzyka; 15) module zadaniowym – należy przez to rozumieć zestawienie przedsięwzięć i zadań przewidzianych do realizacji w sytuacji kryzysowej przez podmioty wskazane w siatce bezpieczeństwa, z wykorzystaniem własnych sił i środków, a także możliwego, zaplanowanego i uzgodnionego wsparcia ze strony innych podmiotów wskazanych w siatce bezpieczeństwa; 19) decyzji 1313/2013/UE – należy przez to rozumieć decyzję Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, z późn. zm.	Wdrożenie rozwiązań zapewniających podstaw zarządzania ryzykiem, z uwzględnieniem postanowień Decyzji Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. Urz. UE L 347 z 20.12.2013, str. 924, L 250 z 04.10.2018, str. 1 oraz L 77A z 20.03.2019, str. 1) – dalej „UMOL” Słowniczek do ustawy uzupełniono o definicje niezbędne m.in. dla opracowania planów zarządzania kryzysowego, zawierających komponent zarzadzania ryzykiem.
Art. 1 pkt 6		Projektowana regulacja przewiduje konieczność opracowania Krajowego Planu Zarządzania Kryzysowego, z uwzględnieniem postanowień UMOL.

	Art. 5e. 1. W celu realizacji zadań z zakresu planowania cywilnego opracowuje się Krajowy Plan Zarządzania Kryzysowego. Rada Ministrów przyjmuje Krajowy Plan Zarządzania Kryzysowego, w drodze uchwały. 2. Krajowy Plan Zarządzania Kryzysowego zawiera: 1) część dotyczącą zarządzania ryzykiem; 2) część dotyczącą reagowania kryzysowego; 3) streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem w rozumieniu decyzji 1313/2013/EU. 3. W części dotyczącej zarządzania ryzykiem Krajowy Plan Zarządzania Kryzysowego zawiera: 1) cele strategiczne; 2) opis zasad współdziałania między podmiotami wskazanymi w siatce bezpieczeństwa; 3) uporządkowaną listę działań na rzecz ograniczenia ryzyka katastrof w zakresie organizacyjnym, technicznym i finansowym, z uwzględnieniem: a) hierarchii działań, b) ram czasowych ich realizacji, c) podmiotów wiodących oraz współpracujących przy ich wykonywaniu, d) sposobów finansowania oraz wysokości nakładów finansowych, e) oceny osiągniętych efektów oraz wniosków z wdrożonych działań. 4. W części dotyczącej reagowania kryzysowego Krajowy Plan Zarządzania Kryzysowego zawiera: 1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków; 2) zasady współdziałania między uczestnikami, o których mowa w pkt 1, w tym wymiany informacji w relacjach krajowych i międzynarodowych; 3) zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych; 4) wykaz modułów zadaniowych pogrupowanych w katalogi; 5) załączniki określające: a) organizację systemu monitorowania zagrożeń, ostrzegania i alarmowania, b) organizację łączności, c) zasady informowania ludności o zagrożeniach i sposobach postępowania na wypadek zagrożeń,	

	d) zasady oraz tryb oceniania i dokumentowania strat i szkód, e) procedury uruchamiania rezerw strategicznych, f) procedury reagowania kryzysowego – standardowe procedury operacyjne, g) priorytety w zakresie ochrony oraz odtwarzania infrastruktury krytycznej, h) wykaz zawartych umów i porozumień związanych z realizacją zadań zawartych w planie reagowania kryzysowego, i) wykaz zawartych umów i porozumień związanych z realizacją zadań ujętych w Krajowym Planie Zarządzania Kryzysowego. 5. Przepis art. 5c ust. 5-11stosuje się odpowiednio. 6. Szef Centrum udostępnia Komisji Europejskiej streszczenie istotnych elementów krajowej oceny zdolności zarządzania ryzykiem, o której mowa w ust. 2 pkt 3.	
Art. 1 pkt 6	"Art. 5g. 1. Plan zarządzania kryzysowego ministra kierującego działem administracji rządowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Centralnego Biura Antykorupcyjnego oraz kierownika urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowanego składa się z części dotyczącej: 1) zarządzania ryzykiem; 2) reagowania kryzysowego. 2. W części dotyczącej zarządzania ryzykiem plan zawiera elementy, o których mowa w art. 5e ust. 3. 3. W części dotyczącej reagowania kryzysowego plan zawiera: 1) określenie zadań i obowiązków uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa w zakresie reagowania w przypadku wystąpienia sytuacji kryzysowej oraz usuwania jej skutków; 2) określenie zadań w zakresie monitorowania zagrożeń; 3) wykaz przedsięwzięć realizowanych w ramach przypisanych katalogów i modułów zadaniowych wraz z ich opisem; 4) określenie organizacji realizacji zadań z zakresu ochrony infrastruktury krytycznej lub zapewnienia ciągłości świadczenia usług kluczowych.	Projektowana regulacja przewiduje konieczność opracowania Krajowego Planu Zarządzania Kryzysowego, z uwzględnieniem postanowień UMOL. Dodatkowo plany zarządzania kryzysowego na pozostałych szczeblach podlegają modyfikacji pod kątem UMOL.

	4. Plan zarządzania kryzysowego, o którym mowa w ust. 1, opracowuje i wdraża minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego oraz kierownik urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany. 5. Minister kierujący działem administracji rządowej, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Agencji Wywiadu, Szef Centralnego Biura Antykorupcyjnego oraz kierownik urzędu centralnego podległego ministrowi kierującemu działem administracji rządowej lub przez niego nadzorowany przekazuje plan zarządzania kryzysowego, o którym mowa w ust. 1, Szefowi Centrum. 6. Minister kierujący działem administracji rządowej, po zasięgnięciu opinii Szefa Centrum, może wydać, w drodze zarządzenia, wytyczne do opracowania planów zarządzania kryzysowego kierowników urzędów centralnych podległych temu ministrowi oraz przez niego nadzorowanych. Art. 5h. 1. Wojewódzki plan zarządzania kryzysowego składa się z części dotyczącej: 1) zarządzania ryzykiem; 2) reagowania kryzysowego. 2. W części dotyczącej zarządzania ryzykiem plan zawiera elementy, o których mowa w art. 5e ust. 3. 3. W części dotyczącej reagowania kryzysowego plan zawiera: 1) elementy, o których mowa w art. 5e ust. 4 pkt 1–3 i 5 oraz art. 5g ust. 3 pkt 2 i 3; 2) wykaz działań określonych planami działań krótkoterminowych, o których mowa w art. 92 ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, wraz z ich opisem; 3) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie województwa wraz z ich opisem; 4) plan ewakuacji ludności, o którym mowa w art. … ustawy …. o ochronie ludności i obronie cywilnej (…) . 4. Wojewoda opracowuje projekt wojewódzkiego planu zarządzania kryzysowego i przekazuje do zatwierdzenia ministrowi właściwemu do spraw administracji publicznej.	

	5. Wojewoda wdraża zatwierdzony wojewódzki plan zarządzania kryzysowego oraz przekazuje go do wiadomości Szefowi Centrum. Art. 5i. 1. Powiatowy plan zarządzania kryzysowego składa się z części dotyczącej: 1) zarządzania ryzykiem; 2) reagowania kryzysowego. 2. W części dotyczącej zarządzania ryzykiem plan zawiera elementy, o których mowa w art. 5e ust. 3. 3. W części dotyczącej reagowania kryzysowego plan zawiera: 1) elementy, o których mowa w art. 5e ust. 4 pkt 1–3 i 5 oraz art. 5g ust. 3 pkt 2 i 3; 2) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem; 3) plan ewakuacji ludności, o którym mowa w art. … ustawy …. o ochronie ludności i obronie cywilnej (…) . 4. Starosta opracowuje projekt powiatowego planu zarządzania kryzysowego i przekazuje do zatwierdzenia właściwemu wojewodzie. 5. Starosta wdraża zatwierdzony powiatowy plan zarządzania kryzysowego. Art. 5j. 1. Gminy plany zarządzania kryzysowego: 1) może składać się z części dotyczącej zarządzania ryzykiem, zawierającej elementy, o których mowa w art. 5e ust. 3; 2) składa się z części dotyczącej reagowania kryzysowego zawierającej: a) elementy, o których mowa w art. 5e ust. 4 pkt 1–3 i 5 oraz art. 5g ust. 3 pkt 2 i 3, b) wykaz przedsięwzięć minimalizujących skutki zakłócenia funkcjonowania usług kluczowych lub infrastruktury krytycznej dla ludności na terenie właściwej jednostki samorządu terytorialnego, wraz z ich opisem, c) plan ewakuacji ludności, o którym mowa w art. … ustawy …. o ochronie ludności i obronie cywilnej (…) . 2. Wójt (burmistrz, prezydent miasta) opracowuje i wdraża gminny plan zarządzania kryzysowego. 3. Wójt (burmistrz, prezydent miasta) przekazuje projekt gminnego planu zarządzania kryzysowego właściwemu staroście.	

	4. Wójt (burmistrz, prezydent miasta) wdraża zatwierdzony gminny plan zarządzania kryzysowego. Art. 5k. 1. Plany zarządzania kryzysowego podlegają systematycznej aktualizacji w cyklu planowania nie dłuższym niż trzy lata. 2. Plany zarządzania kryzysowego uzgadnia się z właściwymi podmiotami, w zakresie ich dotyczącym, planowanymi do wykorzystania przy realizacji przedsięwzięć określonych w planie. 3. Plany postępowania na wypadek wystąpienia sytuacji kryzysowej, opracowane na podstawie odrębnych przepisów, z wyłączeniem planów sporządzanych na czas zewnętrznego zagrożenia bezpieczeństwa państwa i na czas wojny, stanowią załączniki do planu zarządzania kryzysowego właściwego organu administracji publicznej.";	
Art. 1 pkt 8	"Art. 6e. Zadania w zakresie infrastruktury krytycznej obejmują: 1) identyfikację oraz wyznaczanie infrastruktury krytycznej; 2) gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej; 2) opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej; 3) odtwarzanie infrastruktury krytycznej; 4) współpracę między organami administracji publicznej a operatorami infrastruktury krytycznej w zakresie ich ochrony. Art. 6f. 1. Rada Ministrów określi, w drodze uchwały, kryteria pozwalające zidentyfikować obiekty, urządzenia oraz instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi jako infrastrukturę krytyczną, w tym: 1) kryteria sektorowe – progi liczbowe charakteryzujące parametry obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń oraz instalacji, sieci, systemu lub usługi, warunkujące identyfikację infrastruktury krytycznej,	Przepisy dotyczące infrastruktury krytycznej zawierają szereg narzędzi, które w założeniu mają zapewnić maksymalnie efektywną i skuteczną ochronę infrastruktury krytycznej.

	2) kryteria przekrojowe – progi odnoszące się do znaczenia obiektu, urządzenia oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń oraz instalacji, sieci, systemu lub usługi obejmujące: a) kryteria ofiar w ludziach – oceniane w odniesieniu do ewentualnej liczby ofiar śmiertelnych lub liczby rannych, b) kryteria ewakuacji - oceniane w odniesieniu do liczby osób ewakuowanych i czasu ewakuacji, c) kryteria skutków ekonomicznych – oceniane w odniesieniu do znaczenia strat ekonomicznych lub pogorszenia świadczenia jakości usług kluczowych, d) kryteria skutków społecznych – oceniane w odniesieniu do wpływu na zaufanie opinii publicznej oraz zakłócenia codziennego życia obywateli, w tym utraty usług kluczowych, e) kryteria wpływu międzynarodowego – oceniane w odniesieniu do pogorszenia wizerunku kraju na arenie międzynarodowej, możliwości realizacji zobowiązań międzynarodowych, f) kryteria unikatowości - oceniane w odniesieniu do braku możliwości zastąpienia lub odtworzenia w akceptowalnym czasie - uwzględniając znaczenie obiektów, urządzeń oraz instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemów lub usług dla funkcjonowania państwa i zaspokajania potrzeb obywateli, w tym potrzeb lokalnych społeczności oraz świadczenia usług kluczowych. 2. Uchwała, o której mowa w ust. 1, ma charakter niejawny. Art. 6g. 1.Obiekt, urządzenie oraz instalacja lub połączony ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługa mogą zostać wpisane do wykazu infrastruktury krytycznej, jeżeli spełnia łącznie kryterium sektorowe, o którym mowa w art. 6f ust. 1 pkt 1 oraz co najmniej jedno z kryteriów, o których mowa w art. 6f ust. 1 pkt 2. 2. W przypadku infrastruktury krytycznej identyfikowanej przez wojewodów stosuje się kryteria, o których mowa w art. 6f ust. 1 pkt 2. Art. 6h. 1. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda we współpracy z Szefem Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną.	

	2. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda, w sprawie ujęcia obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi, może wystąpić do ich właściciela lub posiadacza o udzielenie informacji, które umożliwią ocenę, czy spełniają one warunki do uznania ich za infrastrukturę krytyczną, przekazując dokumenty niezbędne do udzielenia informacji. 3. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda w wystąpieniu wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot. 4. Minister kierujący działem administracji rządowej oraz właściwy miejscowo wojewoda prowadzą bieżącą wymianę informacji w zakresie realizacji czynności, o których mowa w ust. 1-3. 5. W sytuacjach niecierpiących zwłoki Szef Centrum identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną. Przepisy ust. 2-4 oraz art. 6j ust. 3-6 stosuje się odpowiednio. 6. Komisja Nadzoru Finansowego, w zakresie swojej właściwości, identyfikuje obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieć, system lub usługę mogące stanowić infrastrukturę krytyczną. Przepisy ust. 2-4 oraz art. 6j ust. 3-6 stosuje się odpowiednio. Art. 6i. 1. Szef Centrum prowadzi wykaz infrastruktury krytycznej, który zawiera: 1) nazwę i lokalizację infrastruktury krytycznej; 2) dane operatora infrastruktury krytycznej, w tym siedzibę i adres oraz numer identyfikacji podatkowej (NIP), jeżeli został nadany; 3) wskazanie podmiotu identyfikującego infrastrukturę krytyczną. 2. Wykaz ma charter niejawny. 3. Szef Centrum opracowuje wyciągi z wykazu infrastruktury krytycznej znajdującej się na terenie poszczególnych województw i przekazuje je właściwym wojewodom. Art. 6j. 1. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda, składa do Szefa Centrum wniosek o wpis obiektu, urządzenia,	

	instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi do wykazu infrastruktury krytycznej. Wniosek zawiera informacje, o których mowa w art. 6i. 2. Wniosek sporządza się i składa na piśmie utrwalonym w postaci elektronicznej, opatrzonym kwalifikowanym podpisem elektronicznym, podpisem osobistym albo podpisem zaufanym. 3. Szef Centrum, na podstawie wniosku złożonego przez ministra kierującego działem administracji rządowej dokonuje wpisu do wykazu. Wpis do wykazu jest czynnością materialno-techniczną. 4. Szef Centrum informuje właściciela lub posiadacza obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi o ujęciu w wykazie infrastruktury krytycznej oraz obowiązkach z tym związanych w terminie 30 dni od wpisu do wykazu. 5. Informację, o której mowa w ust. 4, Szef Centrum przekazuje ministrowi kierującemu działem administracji rządowej lub właściwemu miejscowo wojewodzie. 6. Ministrowie kierujący działami administracji rządowej, wojewodowie oraz Szef Centrum w zakresie swojej właściwości zapewniają bieżącą współpracę dotyczącą wyłanianej infrastruktury krytycznej, w tym: 1) prowadzą bieżącą wymianę informacji na temat bieżących zagrożeń; 2) organizują fora ochrony infrastruktury krytycznej; 3) udzielają wsparcia merytorycznego operatorom infrastruktury krytycznej w zakresie wdrażania dobrych praktyk dotyczących ochrony infrastruktury krytycznej. Art. 6k. 1. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda, we współpracy z Szefem Centrum oraz operatorem infrastruktury krytycznej rozpoznaje obiekty, urządzenia, instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi będące w fazie projektowania lub budowy, mogące potencjalnie spełniać kryteria, o których mowa w art. 6f ust. 1, zwane dalej „potencjalną infrastrukturą krytyczną”. Przepisy art. 6h ust. 2 i 3 stosuje się odpowiednio.	

	2. Szef Centrum prowadzi wykaz potencjalnej infrastruktury krytycznej. Przepis art. 6i stosuje się odpowiednio. 3. Minister kierujący działem administracji rządowej lub właściwy miejscowo wojewoda składa do Szefa Centrum wniosek o wpis obiektu, urządzenia, instalacji lub połączonych ze sobą funkcjonalnie obiektów, urządzeń, instalacji oraz sieci, systemu lub usługi do wykazu potencjalnej infrastruktury krytycznej. Wniosek zawiera informacje, o których mowa w art. 6i. Przepisy art. 6j ust. 2-4 stosuje się odpowiednio. 4. Szef Centrum we współpracy z ministrem kierującym działem administracji rządowej lub właściwym terytorialnie wojewodom przedstawia operatorowi infrastruktury krytycznej informacje oraz dokumenty pozwalające na uwzględnienie wymogów dotyczących infrastruktury krytycznej w dokumentacji projektowej lub podczas realizacji inwestycji."; Art. 6l. 1. Operator infrastruktury krytycznej zapewnia jej ochronę, w szczególności przez: 1) prowadzenie systematycznej analizy zagrożeń dla infrastruktury krytycznej; 2) wdrożenie adekwatnych do przeprowadzonej analizy zagrożeń rozwiązań w zakresie: a) bezpieczeństwa fizycznego, w tym ochrony fizycznej oraz zabezpieczeń technicznych, b) bezpieczeństwa osobowego dotyczącego pracowników i dostawców zewnętrznych, c) bezpieczeństwa teleinformatycznego, d) bezpieczeństwa prawnego, e) ciągłości działania i odtwarzania, w tym utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie infrastruktury krytycznej do czasu jej pełnego odtworzenia; 2) bieżącą współpracę z organami administracji publicznej oraz Szefem Centrum przez przekazywanie i odbieranie informacji o: a) zagrożeniach zakłócających lub mogących zakłócić funkcjonowanie infrastruktury krytycznej, b) spodziewanych przerwach lub zakłóceniach w funkcjonowaniu infrastruktury krytycznej;	

	3) sporządzanie i przekazywanie informacji w zakresie zapewnienia ochrony infrastruktury krytycznej odpowiednio na żądanie: a) ministra, o którym mowa w art. 6h, oraz Szefa Centrum, b) właściwego miejscowo wojewody; 4) zapewnienie zdolności do ochrony informacji niejawnych w zakresie realizacji przedsięwzięć związanych z ochroną infrastruktury krytycznej. 2. Operator infrastruktury krytycznej wdraża rozwiązania, o których mowa w ust. 1 pkt 2, z uwzględnieniem minimalnych standardów określonych w przepisach aktu wykonawczego wydanego na podstawie ust. 4 w terminie 6 miesięcy od dnia ujęcia w wykazie infrastruktury krytycznej. 3. Operator infrastruktury krytycznej może, w celu zapewnienia wdrożenia rozwiązań, o których mowa w ust. 1 pkt 1, żądać od usługodawców w postępowaniach przetargowych lub zamówieniach: 1) zdolności do ochrony informacji niejawnych oraz stosowania tych przepisów przy projektowaniu i wykonywaniu obiektów, urządzeń instalacji i innych systemów będących elementami infrastruktury krytycznej; 2) certyfikatów potwierdzających posiadanie właściwych kompetencji i uprawnień wskazanych w akcie wykonawczym wydanym na podstawie art. 6zf ust. 9. 4. Rada Ministrów określi, w drodze rozporządzenia minimalne standardy ochrony infrastruktury krytycznej uwzględniając bezpieczeństwo fizyczne, techniczne, osobowe, teleinformatyczne, prawne oraz ciągłość działania z uwzględnieniem lokalizacji i charakterystyki infrastruktury krytycznej. Art. 6m. 1. Operator infrastruktury krytycznej opracowuje, stosuje i aktualizuje dokumentację ochrony infrastruktury krytycznej. 2. Dokumentację, o której mowa w ust. 1, zawiera: 1) charakterystykę infrastruktury krytycznej oraz analizę zagrożeń, o której mowa w art. 6l ust. 1 pkt 1; 2) opis zastosowanych, adekwatnie do rodzaju zagrożeń środków bezpieczeństwa w zakresie zapewnienia: a) bezpieczeństwa fizycznego, w tym opis organizacji i wykonywania ochrony fizycznej infrastruktury krytycznej, w tym dane specjalistycznej uzbrojonej formacji ochronnej chroniącej infrastrukturę krytyczną, o której mowa w art. 2 pkt 7 ustawy	

	z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2021 r. poz. 1995) – jeżeli występuje, b) bezpieczeństwa technicznego, c) bezpieczeństwa osobowego, d) bezpieczeństwa teleinformatycznego, e) bezpieczeństwa prawnego, f) ciągłości działania i odtwarzania; 4) opis: a) zasobów umożliwiających podtrzymanie funkcjonowania infrastruktury krytycznej do czasu jej pełnego odtworzenia, b) współpracy z właściwymi podmiotami administracji publicznej dotyczący wymiany informacji o zdarzeniu zakłócającym lub mogącym zakłócić funkcjonowanie infrastruktury krytycznej oraz sposobu postępowania w przypadku takiego zdarzenia; 5) procedury: a) działania w sytuacji zagrożenia lub zakłócenia funkcjonowania infrastruktury krytycznej, b) zapewnienia ciągłości funkcjonowania infrastruktury krytycznej, c) odtwarzania infrastruktury krytycznej; 6) inne elementy niż wskazane w pkt 1-5, biorąc pod uwagę charakterystykę infrastruktury krytycznej. 3. Operator infrastruktury krytycznej uzgadnia z właściwymi podmiotami administracji publicznej zakres współpracy, o której mowa w ust. 2 pkt 5 lit. a. 4. Do dokumentacji ochrony infrastruktury krytycznej stosuje się przepisy o ochronie informacji niejawnych lub o ochronie tajemnicy przedsiębiorstwa. 5. Operator infrastruktury krytycznej w terminie 6 miesięcy od uzyskania informacji o ujęciu w wykazie infrastruktury krytycznej przedkłada oświadczenie o opracowaniu dokumentacji ochrony infrastruktury krytycznej oraz wdrożeniu minimalnych wymagań, o których mowa w art. 6l ust. 4, odpowiednio: 1) ministrowi, o którym mowa w art. 6h, oraz Szefowi Centrum; 2) właściwemu miejscowo wojewodzie. 6. W przypadku braku możliwości wdrożenia rozwiązań, o których mowa w art. 6l ust. 1 pkt 2, z uwzględnieniem minimalnych standardów określonych w przepisach	

	aktu wykonawczego wydanego na podstawie art. 6l ust. 4, dokumentacja, o której mowa w art. 6m podlega uzgodnieniu odpowiednio z: 1) ministrem, o którym mowa w art. 6h lub Szefem Centrum; 2) właściwym miejscowo wojewodą. 7. Minister, o którym mowa w art. 6h, Szef Centrum oraz właściwym miejscowo wojewoda mogą wskazać podmioty administracji publicznej, od których operator ma uzyskać opinię na temat sporządzonej dokumentacji oraz określają termin do zasięgnięcia opinii. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania informacji przez operatora infrastruktury krytycznej o konieczności zasięgnięcia opinii. 8. Operator infrastruktury krytycznej będący jednocześnie operatorem usługi kluczowej w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa uwzględnia w dokumentacji, o której mowa w ust. 1, dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, określoną w przepisach wydanych na podstawie art. 10 ust. 5 tej ustawy. Art. 6n. 1. Operator infrastruktury krytycznej sporządza, w terminie do dnia 31 marca każdego roku raport o stanie ochrony infrastruktury krytycznej za rok ubiegły. 2. Raport o stanie ochrony infrastruktury krytycznej zawiera w szczególności informacje dotyczące jej ochrony w zakresie zapewnienia: 1) bezpieczeństwa fizycznego; 2) bezpieczeństwa technicznego; 3) bezpieczeństwa osobowego; 4) bezpieczeństwa teleinformatycznego; 5) bezpieczeństwa prawnego; 6) ciągłości działania i odtwarzania. 3. Raport o stanie ochrony infrastruktury krytycznej sporządza się z uwzględnieniem: 1) analizy zagrożeń dla infrastruktury krytycznej, o której mowa w art. 6l ust. 1 pkt 1; 2) wdrożonych rozwiązań, o których mowa w art. 6l ust. 1 pkt 2; 3) zagrożeń, które zakłóciły lub mogły zakłócić funkcjonowanie infrastruktury krytycznej, a nie były uwzględnione w analizie, o której mowa w art. 6l ust. 1 pkt 1;	

	4) wyników przeprowadzonych kontroli i audytów odnoszących się do wdrożonych rozwiązań, o których mowa w art. 6l ust. 1 pkt 2; 5) opisu działań podjętych przez operatora infrastruktury krytycznej w przypadkach wystąpienia zagrożeń. 4. Operator infrastruktury krytycznej przekazuje, w terminie do dnia 31 marca każdego roku, raport o stanie ochrony infrastruktury krytycznej ministrowi odpowiednio: 1) ministrowi, o którym mowa w art. 6h oraz Szefowi Centrum; 2) właściwemu miejscowo wojewodzie. 5. Raport o stanie ochrony infrastruktury krytycznej sporządza się z zachowaniem przepisów o ochronie informacji niejawnych. Art. 6o. 1. W celu realizacji zadań, o których mowa w art. 6l - 6n, operator infrastruktury krytycznej wyznacza koordynatora do spraw ochrony infrastruktury krytycznej, zwanego dalej „koordynatorem”. 2. Operator infrastruktury krytycznej wyznacza koordynatora w terminie 30 dni od dnia otrzymania informacji o ujęciu w wykazie infrastruktury krytycznej. 3. Koordynatorem może być osoba, która: 1) jest pracownikiem operatora infrastruktury krytycznej albo żołnierzem lub funkcjonariuszem pełniącym służbę w jednostce organizacyjnej będącej operatorem infrastruktury krytycznej; 2) korzysta z pełni praw publicznych; 3) posiada wiedzę, umiejętności i doświadczenie w zakresie zarządzania bezpieczeństwem, z uwzględnieniem przedmiotu działalności operatora infrastruktury krytycznej; 4) nie była skazana prawomocnym wyrokiem za umyślne przestępstwo lub umyślne przestępstwo skarbowe; 5) spełnia wymagania bezpieczeństwa osobowego w zakresie dostępu do informacji niejawnych o klauzuli co najmniej „poufne”. 4. Koordynator podlega bezpośrednio organowi zarządzającemu operatora infrastruktury krytycznej. 5. O wyznaczeniu koordynatora operator infrastruktury krytycznej informuje odpowiednio:	

	1) ministra, o którym mowa w art. 6h oraz Szefa Centrum; 2) właściwego miejscowo wojewodę. 6. Operator infrastruktury krytycznej zapewnia koordynatorowi organizacyjne i techniczne warunki realizacji zadań, o których mowa w art. 6l – 6n, w tym dostęp do niezbędnych dokumentów i informacji. Art. 6p. 1. W przypadku pracownika zatrudnionego na stanowisku umożliwiającym dostęp do informacji o bezpieczeństwie obiektu infrastruktury krytycznej i osoby ubiegającej się o zatrudnienie na tym stanowisku, operator infrastruktury krytycznej żąda od pracownika i tej osoby przedłożenia informacji dotyczących karalności, w tym informacji, czy ich dane osobowe są zgromadzone w Krajowym Rejestrze Karnym. 2. Operator infrastruktury krytycznej żąda od pracownika danych biometrycznych w postaci odcisków linii papilarnych palców, głosu, obrazu rogówki, sieci żył palców lub biometrii twarzy, jeżeli podanie takich danych jest konieczne ze względu na kontrolę dostępu do informacji o bezpieczeństwie obiektu infrastruktury krytycznej i pomieszczeń. 3. Operator infrastruktury krytycznej przechowuje informacje i dane, o których mowa w ust. 1 i 2, wyłącznie przez okres zatrudnienia pracownika, którego te dane dotyczą."; 	
Art. 1 pkt 10 i 11	w art. 7a w ust. 2 pkt 1 otrzymuje brzmienie: "1) zapewnienia właściwego funkcjonowania, ochrony, wzmocnienia oraz odbudowy infrastruktury krytycznej lub niezakłóconego świadczenia usługi kluczowej;"; w art. 7ba w ust. 2 pkt 1 otrzymuje brzmienie: "1) zapewnienia właściwego funkcjonowania, ochrony, wzmocnienia oraz odbudowy infrastruktury krytycznej lub niezakłóconego świadczenia usługi kluczowej;";	Zmiany wynikowe do regulacji związanych ze świadczeniem usługi kluczowej przez podmiot krytyczny.

Art. 1 pkt 12	w art. 10 ust. 2-3 otrzymują brzmienie: "2. Centrum kieruje Szef powoływany i odwoływany przez Prezesa Rady Ministrów. 2a. Szef Centrum pełni funkcję sekretarza Zespołu, o którym mowa w art. 8 ust. 1. 3. Zastępców Szefa Centrum powołuje i odwołuje Prezes Rady Ministrów, na wniosek Szefa Centrum.";	
Art. 1 pkt 13	dodaje się art. 11b - 11 e w brzmieniu: "Art. 11b.W celu realizacji zadań planowania cywilnego wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego, Centrum: 1) koordynuje: a) udział przedstawicieli Rzeczypospolitej Polskiej w pracach Komitetu Odporności NATO oraz zapewnia wsparcie merytoryczne prowadzonych prac, b) opracowywanie stanowisk Rzeczypospolitej Polskiej na potrzeby: - procesów planowania obronnego Organizacji Traktatu Północnoatlantyckiego, - cyklicznych przeglądów systemu reagowania kryzysowego Organizacji Traktatu Północnoatlantyckiego, c) uruchamianie przedsięwzięć i procedur systemu zarzadzania kryzysowego; 2) zapewnia funkcjonowanie Narodowego Punktu Kontaktowego w ramach systemu reagowania kryzysowego Organizacji Traktatu Północnoatlantyckiego. Art. 11c. 1. Szef Centrum zapewnia funkcjonowanie systemu teleinformatycznego wykorzystywanego jako narzędzie wspierające realizację zadań zarządzania kryzysowego, zwanego dalej „systemem". 2. System zapewnia możliwość: 1) zgłaszania informacji o potencjalnych zagrożeniach oraz zaistniałych zagrożeniach; 2) gromadzenie informacji o zagrożeniach oraz analizę tych informacji; 3) gromadzenie informacji o siłach i środkach niezbędnych do realizacji zadań zarządzania kryzysowego; 4) agregowanie i korelowanie pozyskiwanych informacji. 3. Użytkownikami systemu są:	

	1) ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych podległych ministrom kierującym działami administracji rządowej lub przez nich nadzorowanych; 2) wojewodowie; 3) starostowie. 4. Użytkownikami systemu mogą być wójtowie, burmistrzowie, prezydenci miast. 5. Podmioty, o których mowa w ust. 3 i 4, przekazują do systemu informacje o potencjalnych zagrożenia oraz zaistniałych zagrożeniach niezwłocznie po uzyskaniu takich informacji. 6. Administratorem danych osobowych przetwarzanych w systemie jest Szef Centrum. 7. Przetwarzanie danych osobowych zgromadzonych w systemie nie wymaga realizacji obowiązków, o których mowa w art. 12-22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1). W systemie nie gromadzi się danych osobowych szczególnej kategorii. 8. Dane osobowe zgromadzone w systemie podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu i są przechowywane wyłącznie przez okres niezbędny do realizacji zadań. Art. 11d. 1. Informacje z systemu są udostępniane użytkownikom systemu, o których mowa w art. 11c ust. 3 i 4. 2. Informacje z systemu udostępnia się na wniosek, o ile są one niezbędne do realizacji ich ustawowych zadań, innym podmiotom niż wskazane w art. 11c ust. 3 i 4. Art. 11e. Rada Ministrów określi w drodze rozporządzenia: 1) zakres informacji przekazywanych do systemu przez jego użytkowników, oraz sposób i tryb ich wprowadzania; 2) zakres informacji, do których zapewnia się dostęp użytkownikom systemu;	

	3) sposób funkcjonowania systemu; 4) sposób i tryb zakładania i obsługi konta użytkowników systemu, 5) wymogi bezpieczeństwa teleinformatycznego, które muszą spełnić podmioty krajowego systemu, aby uzyskać dostęp do systemu, o którym mowa w …(w zakresie np. danych osobowych) - uwzględniając konieczność zapewnienia sprawnego wykonywania zadań zarzadzania kryzysowego oraz zapewnienia odpowiedniego poziomu bezpieczeństwa danych zgromadzonych w systemie.";	
Art. 1 pkt 14	w art. 12: a) ust. 1 otrzymuje brzmienie: „1. Ministrowie kierujący działami administracji rządowej oraz kierownicy urzędów centralnych realizują, w zakresie swojej właściwości, zadania dotyczące zarządzania kryzysowego, w tym: 1) opracowują plany zarządzania kryzysowego; 2) organizują, prowadzą i koordynują szkolenia i ćwiczenia z zakresu zarządzania kryzysowego oraz biorą udział w ćwiczeniach krajowych i międzynarodowych; 3) współpracują z operatorami infrastruktury krytycznej lub podmiotami krytycznymi w zakresie realizacji zadań ochrony infrastruktury krytycznej oraz zapewnienia niezakłóconego świadczenia usług kluczowych; 4) zapewniają funkcjonowania stałego dyżuru w ramach podwyższania gotowości obronnej państwa", b) uchyla się ust. 2 i 2a, c) ust. 2c otrzymuje brzmienie: „2c. Do zadań zespołów, o których mowa w ust. 2b, należy: 1) dokonywanie okresowej oceny ryzyka na potrzeby Krajowej Oceny Ryzyka; 2) dokonywanie okresowej oceny gotowości do reagowania w przypadku wystąpienia sytuacji kryzysowej w zakresie organizacyjnym, technicznym i finansowym; 3) opiniowanie projektów planów zarządzania kryzysowego; 4) opiniowanie wykazu infrastruktury krytycznej w ramach swojej właściwości; 5) wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom.”;	

Art. 1 pkt 15	w art. 13 uchyla się ust. 2a	
Art. 1 pkt 16	w art. 14: a) w ust. 2 pkt 7 otrzymuje brzmienie: "7) organizacja wykonania zadań z zakresu ochrony infrastruktury krytycznej lub zapewnienia niezakłóconego świadczenia usług kluczowych.", b) ust. 4 otrzymuje brzmienie: "4. Minister właściwy do spraw administracji publicznej, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii Szefa Centrum, wydaje, w drodze zarządzenia, wojewodom wytyczne do wojewódzkich planów zarządzania kryzysowego.";	
Art. 1 pkt 17	art. 20b otrzymuje brzmienie: "Art. 20b. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych, wojewodowie, starostowie, wójtowie (burmistrzowie, prezydenci miast), operatorzy infrastruktury są obowiązani do udzielania Szefowi Centrum, w wyznaczonym terminie, żądanych przez niego informacji i wyjaśnień niezbędnych do realizacji zadań Centrum określonych w ustawie.”;	
Art. 1 pkt 18	art. 21a otrzymuje brzmienie: "Art. 21a. 1. Ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie niezwłocznie informują Szefa Centrum o zagrożeniu, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej, oraz o konieczności powiadomienia ludności o zagrożeniu. 2. Operatorzy infrastruktury krytycznej niezwłocznie informują Szefa Centrum oraz właściwe wojewódzkie centrum zarządzania kryzysowego o zakłóceniu funkcjonowania tej infrastruktury, które może skutkować wystąpieniem na wskazanym obszarze sytuacji kryzysowej.	

	3. Operator ruchomej publicznej sieci telekomunikacyjnej w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648 i 1933), zwany dalej „operatorem”, jest obowiązany, na żądanie Szefa Centrum, do niezwłocznego, nieodpłatnego wysłania lub wysyłania, komunikatów do wszystkich lub określonych przez Szefa Centrum grup użytkowników końcowych, w szczególności przebywających na określonym przez niego obszarze, jednorazowo lub przez wskazany przez Szefa Centrum okres. 4. Obowiązek, o którym mowa w ust. 3, nie obejmuje wysłania lub wysyłania komunikatu użytkownikom końcowym, których karty SIM są zainstalowane i wykorzystywane w urządzeniach telemetrycznych. 5. Operator po wysłaniu komunikatu niezwłocznie przekazuje dyrektorowi Centrum informację o liczbie kart SIM użytkowników końcowych, do których komunikat został wysłany i którym komunikat został dostarczony. 6. Rada Ministrów określi, w drodze rozporządzenia, sposób i tryb współpracy dyrektora Centrum z operatorem w celu realizacji obowiązku, o którym mowa w ust. 3, niezbędne elementy komunikatu oraz sposób jego przekazywania użytkownikom końcowym, mając na uwadze konieczność: 1) zapewnienia efektywnego i niezakłóconego przepływu informacji między Centrum a operatorem; 2) zapewnienia sprawnej dystrybucji komunikatu na obszarze zagrożonym wystąpieniem sytuacji kryzysowej oraz łatwości zrozumienia treści zawartych w komunikacie i zastosowania się do nich.";	
Art. 1 pkt 20	w art. 26 po ust. 4 dodaje się ust. 4a w brzmieniu: „4a. Środki finansowe z rezerwy celowej, o której mowa w ust. 4, mogą być przeznaczone na realizację przedsięwzięć związanych z zarządzaniem ryzykiem oraz reagowaniem w przypadku wystąpienia sytuacji kryzysowej oraz usuwaniem jej skutków i odtwarzaniem zasobów.”;	

Art. 2	Art. 2. W ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2018 r. poz. 2142 i 2245 oraz z 2019 r. poz. 1495) w art. 5 w ust. 2 pkt 5 otrzymuje brzmienie: „5) obiekt, urządzenie, instalację lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi ujęte w wykazie w wykazie, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r. poz. 1398 oraz z 2020 r. poz. …).”.	Zmiany wynikowe do zmian w ustawie o zarządzaniu kryzysowym, głównie w zakresie odniesień do nowych definicji, dokumentów rządowych lub zmiany terminologii z Dyrektora Centrum na Szefa Centrum.
Art. 3.	W ustawie z dnia 29 listopada 2000 r. - Prawo atomowe (Dz. U. z 2023 r. poz. 1890 oraz z 2024 r. poz. 834) w art. 41o pkt 4 otrzymuje brzmienie: "4) Szef Rządowego Centrum Bezpieczeństwa - w zakresie zarządzania kryzysowego, ochrony infrastruktury krytycznej oraz monitorowania potencjalnych zagrożeń w rozumieniu przepisów ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 …);".	j.w.
Art. 4.	Art. 4. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812) wprowadza się następujące zmiany: 1) w art. 5 w ust. 1 pkt 2a otrzymuje brzmienie: „2a) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz …), a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy;”; 2) w art. 32a ust. 1 otrzymuje brzmienie: „1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazem, o którym mowa w art. 6i ust. 1 ustawy z	j.w.

	dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców ABW może przeprowadzać ocenę bezpieczeństwa tych systemów teleinformatycznych, zwaną dalej „oceną bezpieczeństwa”.”; 3) w art. 32aa ust. 1 otrzymuje brzmienie: „1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych wykazami, o których mowa w art. art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a także systemów teleinformatycznych operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a tej ustawy, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców ABW wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania”, prowadzi go i koordynuje jego funkcjonowanie.”.	
Art. 5	Art. 5. W ustawie z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2019 r. poz. 692) w art. 24 ust. 5 otrzymuje brzmienie: „5. W przypadku wprowadzenia poziomu ochrony 3 stosuje się odpowiednio art. 21 i art. 25 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U z 2023 r. poz. 122 oraz …).”.	j.w.

Art. 6	Art. 6. W ustawie z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2020 r. poz. 2173 oraz z 2024 r. poz. 834) wprowadza się następujące zmiany: 1) w art. 1 ust. 1 otrzymuje brzmienie: „1. Ustawa określa szczególne uprawnienia przysługujące ministrowi właściwemu do spraw aktywów państwowych w spółkach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w wykazie, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz …), zwanych dalej „spółkami”.”; 2) w art. 5 ust. 4 otrzymuje brzmienie: „4. Pełnomocnik do spraw ochrony infrastruktury krytycznej może być koordynatorem do spraw ochrony infrastruktury krytycznej, o którym mowa w art. 6o ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”; 3) w art. 4 ust.1, art. 5 ust. 1 i ust. 2 pkt 5 i 6, art. 6 ust. 4-6 wyraz "dyrektor" zastępuje się wyrazem "Szef".".	j.w.
Art. 7	Art. 7. W ustawie z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2019 r. poz. 701, 730, 1403 i 1579) w art. 25 w ust. 6i pkt 2 otrzymuje brzmienie: „2) stanowiącego element infrastruktury krytycznej ujętej w wykazie, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz …);”.	j.w.

Art. 8	Art. 8. W ustawie z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2024 r. poz. 383) w art. 4 w pkt 8 lit. b otrzymuje brzmienie: „b) obiekty, urządzenia, instalacje lub połączone ze sobą funkcjonalnie obiekty, urządzenia, instalacje oraz sieci, systemy lub usługi ujęte w wykazie infrastruktury krytycznej, o którym mowa w art. 6i ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz …);”.	j.w.
Art. 9	Art. 9. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 oraz z 2019 r. poz. 2020 i 2248) wprowadza się następujące zmiany: 1) w art. 10 w ust. 4 wyrazy ,,właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami ,,operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”; 2) w art. 15 w ust. 7 w pkt 2 wyrazy ,,właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1” zastępuje się wyrazami ,,operatorem infrastruktury krytycznej, o którym mowa w art. 3 pkt 3a”; 3) w art. 26: a) w ust. 2 wyrazy ,,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” zastępuje się wyrazami ,,operatorów infrastruktury krytycznej, o których mowa w art. 3 pkt 3a”, b) w ust. 5 pkt 1 otrzymuje brzmienie: „1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne	j.w.

	objęte są wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;”, c) w ust. 7 pkt 5 i 6 otrzymują brzmienie: „5) inne niż wymienione w pkt 1–4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych wykazami, o których mowa w art. 5c pkt 1 i art. 5d ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.”.	
Art. 10	Art. 10. W ustawie z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2023 r. poz. 294) wprowadza się następujące zmiany: 1) w art. 2: a) pkt 1 otrzymuje brzmienie: "1) infrastruktura krytyczna - infrastrukturę, o której mowa w art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz …), b) dodaje się pkt 1a i 1b w brzmieniu: "1a) podmiot krytyczny - podmiot, o którym mowa w art. 3 pkt 1a ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 1b) usługa kluczowa - usługa, o której mowa w art. 3 pkt 1d ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;"; 2) w art. 8: a) w ust. 2 pkt 21 otrzymuje brzmienie:	j.w.

	"21) Szefem Rządowego Centrum Bezpieczeństwa;", b) w ust. 4 pkt 1 i 2 otrzymują brzmienie: "1) ocenę ryzyka zidentyfikowanych zagrożeń oraz sposobów i środków reagowania na zagrożenia, z uwzględnieniem rozwiązań zawartych w planie zarządzania kryzysowego, o którym mowa w art. 5g ust. 1 ustawy o zarządzaniu kryzysowym; 2) wnioski wynikające z wykonania postanowień Strategii Oporności Podmiotów Krytycznych, o której mowa w art. 5f ustawy o zarządzaniu kryzysowym, w zakresie sprawowania nadzoru nad infrastrukturą krytyczną oraz podmiotami krytycznymi zapewniającymi świadczenie usług kluczowych;"; 3) w art. 9 w ust. 1 pkt 1 otrzymuje brzmienie: „1) wnioski dotyczące tworzenia, utrzymywania i likwidacji rezerw wynikające z oceny ryzyka zidentyfikowanych zagrożeń zawartej w Krajowej Ocenie Ryzyka, o której mowa w art. 5c ustawy o zarządzaniu kryzysowym, oraz wnioski, o których mowa w art. 8 ust. 4 pkt 2;".	
Art. 11	Art. 11. W ustawie z dnia 27 stycznia 2023 r. o kontroli niektórych inwestycji (Dz. U. z 2023 r. poz. 415 oraz z 2024 r. poz. 834) w art. 13 w ust. 3 pkt 22 otrzymuje brzmienie: "22) Szefa Rządowego Centrum Bezpieczeństwa.".	j.w.
Art. 12	Art. 12. W ustawie z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. 1703) art. 15 otrzymuje brzmienie: „Art. 15. W zakresie dotyczącym współpracy Szefa Rządowego Centrum Bezpieczeństwa z operatorem ruchomej publicznej sieci telekomunikacyjnej w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne przy realizacji obowiązków określonych w art. 21a ust. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2023 r. poz. 122 oraz …), przepisów art. 10-14 nie stosuje się.”.	j.w.