# Ustawa o Krajowym Systemie Cyberbezbieczeństwa

Krzysztof Silicki

Zastępca Dyrektora NASK PIB,
Dyrektor ds. Cyberbezpieczeństwa i Innowacji
Wiceprzewodniczący Rady Zarządzającej ENISA

# Projekt ustawy o KSC – co to jest?

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) zapewnia implementację dyrektywy NIS*
- Ustanawia ramy prawne funkcjonowania KSC
- Rozszerza obszar oddziaływania w stosunku do dyrektywy NIS, np.:
  - włącza sektor administracji publicznej,
  - nakłada obowiązek zgłaszania incydentów które MOGĄ spowodować negatywny skutek (nie tylko te, które coś spowodowały)
- Projekt ustawy jest przed drugim czytaniem w Sejmie

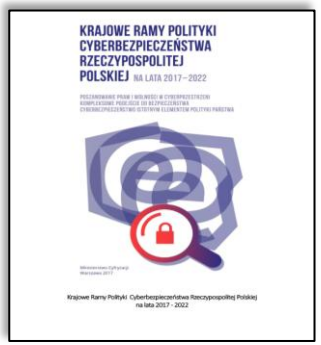
Ważne: uoKSC w obszarze administracji publicznej jest dodatkowym komponentem bezpieczeństwa teleinformatycznego ustanowionym przez ustawę o informatyzacji (…) i Krajowe Ramy Interoperacyjności

* Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

# Dyrektywa NIS

**Wybrane obowiązki nałożone na państwa członkowskie:**

- Identyfikacja **operatorów usług kluczowych w kilku sektorach** oraz określenie wymagań bezpieczeństwa teleinformatycznego.
- Wyznaczenie **organów właściwych** dla operatorów usług kluczowych i dostawców usług cyfrowych.
- Wyznaczenie **pojedynczego punktu kontaktowego.**
- Wyznaczenie **CSIRT*** dla operatorów usług kluczowych i dostawców usług cyfrowych.
- Wymiana informacji i **raportowanie** na poziomie UE na temat **poważnych incydentów** u operatorów usług kluczowych oraz **istotnych incydentów** u dostawców usług cyfrowych.
- Przyjęcie w unijnej **procedurze komitetowej** wymagań dla dostawców usług cyfrowych.
- Przyjęcie krajowej **strategii** bezpieczeństwa sieci i informacji.




*zespół reagowania na incydenty bezpieczeństwa komputerowego

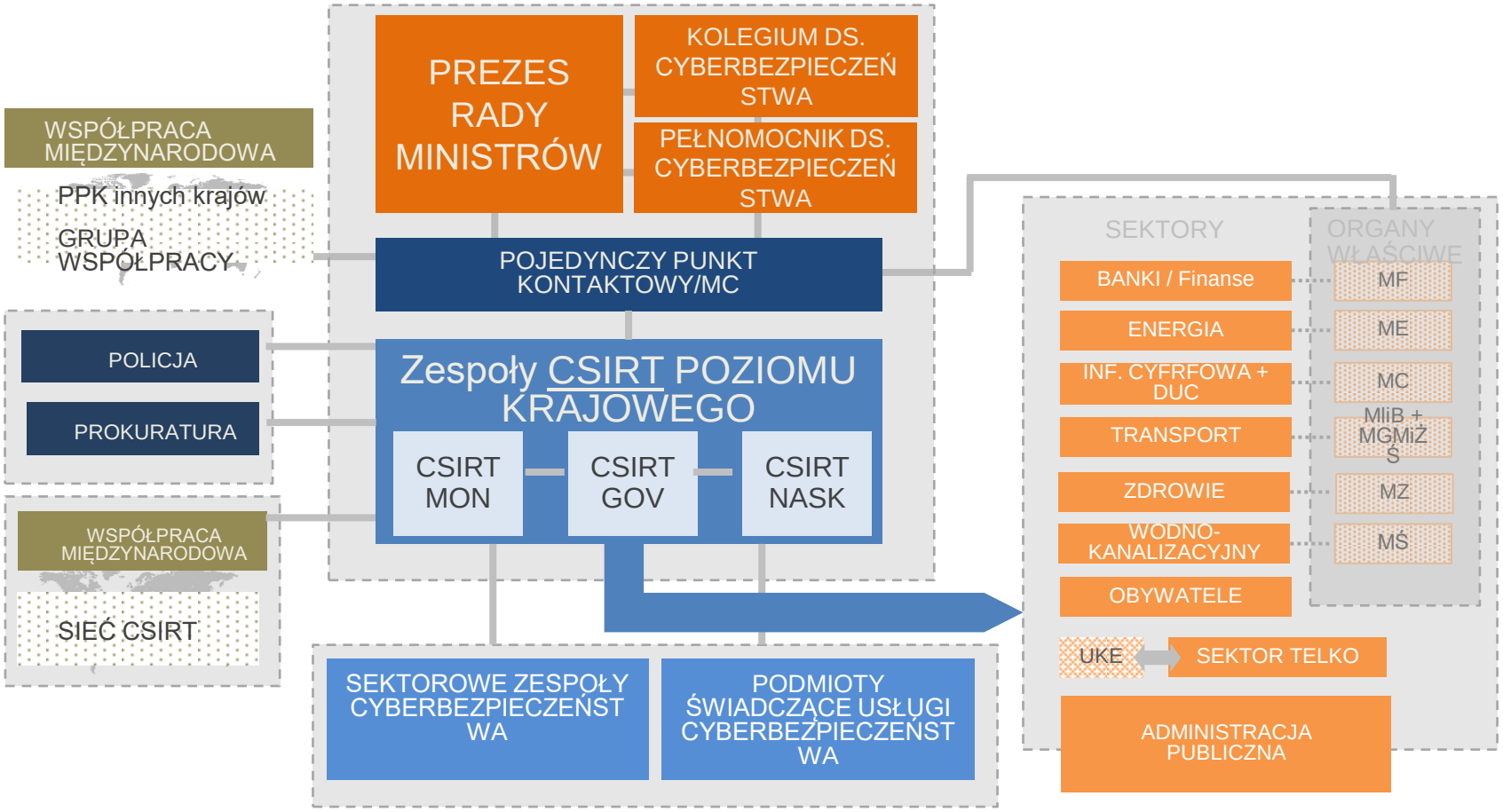
# Ustawa o KSC: definicje

*Pojęcia podstawowe dotyczące incydentu:*

- **incydent w podmiocie publicznym** – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny
- **incydent krytyczny** – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi,
- **obsługa incydentu** – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych, ograniczenie skutków incydentu
- **zarządzanie incydentem** – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowanie wniosków z obsługi incydentu;

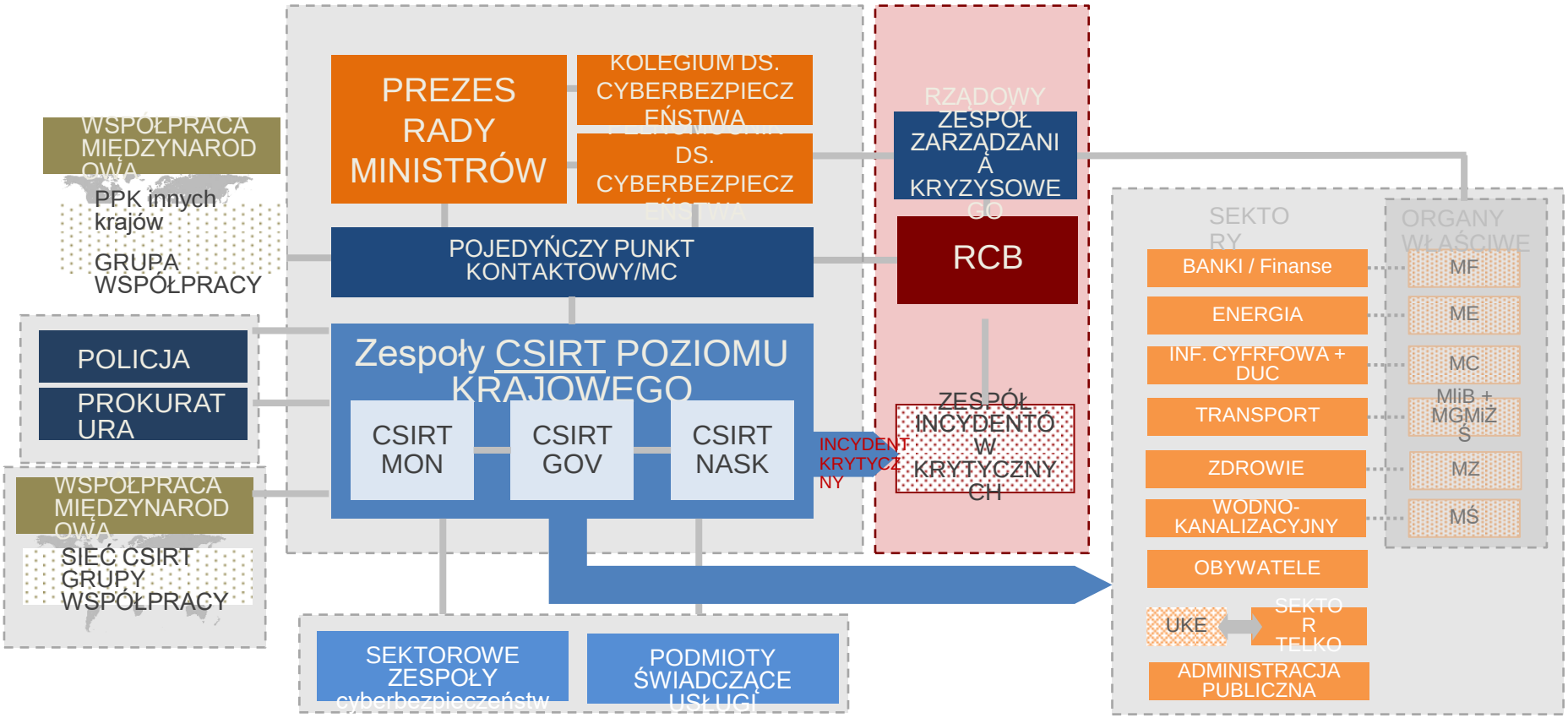
# Architektura KSC

ARCHITEKTURA Krajowego SYSTEMU CYBERBEZPIECZEŃSTWA



# Obsługa incydentów krytycznych

PROCES OBSŁUGI INCYDENTÓW KRYTYCZNYCH



# Constituency CSIRT NASK

W obszarze odpowiedzialności CSIRT NASK są między innymi:

- jednostki samorządu terytorialnego oraz ich związki;
- związki metropolitalne;
- jednostki budżetowe;
- samorządowe zakłady budżetowe;
- agencje wykonawcze;
- instytucje gospodarki budżetowej;
- spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,

# Obowiązki administracji publicznej

*Osoba do kontaktów:*

- Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do **wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów** z podmiotami krajowego systemu cyberbezpieczeństwa.

- Organ administracji publicznej **może wyznaczyć jedną osobę odpowiedzialną** za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych **przez jednostki jemu podległe lub przez niego nadzorowane.**

- Jednostka samorządu terytorialnego **może wyznaczyć jedną osobę odpowiedzialną** za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, **realizowanych przez jej jednostki organizacyjne.**

# Obowiązki administracji publicznej

*Obsługa i zgłaszanie incydentów:*

Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego:

- **zapewnia zarządzanie incydentem** w podmiocie publicznym;
- **zgłasza incydent niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia**, do właściwego CSIRT;
- zgłoszenie przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.
- zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego **we współpracy z właściwym CSIRT,** przekazując niezbędne dane, w tym dane osobowe;

# Obowiązki administracji publicznej

*Co zawiera zgłoszenie incydentu:*

- dane podmiotu zgłaszającego,
- dane osoby składającej zgłoszenie;
- dane osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
- **opis wpływu incydentu** w podmiocie publicznym na realizowane zadanie publiczne, w tym:
  - wskazanie zadania publicznego, na które incydent miał wpływ,
  - liczbę osób, na które incydent miał wpływ,
  - moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
  - zasięg geograficzny, którego dotyczy incydent,
  - przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
  - informacje o podjętych działaniach zapobiegawczych;
  - informacje o podjętych działaniach naprawczych;
  - inne istotne informacje.

# Obowiązki administracji publicznej

*Przekazywanie i uzupełnianie danych incydentu:*

- Podmiot publiczny, przekazuje **informacje znane w chwili zgłoszenia, które uzupełnia w trakcie obsługi incydentu**
- Mogą być przekazywane informacje stanowiące **tajemnice prawnie chronione** gdy jest to konieczne dla realizacji zadań, właściwego CSIRT
- W zgłoszeniu podmiot publiczny oznacza informacje stanowiące tajemnice prawnie chronione
- CSIRT może zwrócić się do podmiotu publicznego o **uzupełnienie zgłoszenia** o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań związanych z incydentem

# Obowiązki administracji publicznej

*Dobrowolne zgłoszenia:*

*Oprócz zgłoszeń obowiązkowych, o których mowa wcześniej, można do właściwego CSIRT przekazywać informacje:*

- o innych incydentach;
- o zagrożeniach cyberbezpieczeństwa;
- dotyczące szacowania ryzyka;
- o podatnościach;
- o wykorzystywanych technologiach.

# Obowiązki administracji publicznej

*Informowanie:*

Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego:

- zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, **dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa** i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

- przekazuje do właściwego CSIRT **dane osoby do kontaktów**, zawierające imię i nazwisko, numer telefonu, adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

# Wsparcie i korzyści dla administracji publicznej

Podstawowe zadania CSIRT

- CSIRTy monitorują zagrożenia cyberbezpieczeństwa i incydenty na poziomie krajowym;
- Reagują na zgłoszone incydenty
- Dokonują szacowania ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami;

Wsparcie dla podmiotów

CSIRTy:

- **przekazują informacje dotyczące incydentów i ryzyk** podmiotom krajowego systemu cyberbezpieczeństwa;
- **wydają komunikaty o zidentyfikowanych zagrożeniach** cyberbezpieczeństwa

CSIRT w uzasadnionych przypadkach może zapewnić **wsparcie w obsłudze incydentów**

CSIRT może przekazywać **informacje o podatnościach i sposobie ich usunięcia** w wykorzystywanych technologiach

# Obowiązki administracji publicznej

*Podmiot publiczny może być **jednocześnie operatorem usługi kluczowej:***

Do podmiotu publicznego wobec którego wydana została **decyzja o uznaniu za operatora usługi kluczowej**, stosuje się przepisy w zakresie świadczenia usługi kluczowej, w związku ze świadczeniem której został uznany za operatora usługi kluczowej.

***Podmiot staje się operatorem usługi kluczowej i podlega regułom narzuconym przez dyrektywę NIS i uoKSC:***

- ***wdrażanie środków bezpieczeństwa proporcjonalnych do analizy ryzyka,***
- ***przeprowadzania cyklicznych audytów,***
- ***Prowadzenia dokumentacji bezpieczeństwa,***
- ***zgłaszania do CSIRT poważnych incydentów (wg. określonych kryteriów i progów)***
- ***poddawania się kontroli ze strony właściwego organu ds. cyberbezpieczeństwa***

# Samorządy a kluczowe sektory

*Decyzja o uznaniu za operatora usługi kluczowej*

- Może to dotyczyć takich sektorów jak:
  - wodno-kanalizacyjny
  - zdrowia
  - transportu (np. kolejowego)
  - energetyczny

- Wpisanie do wykazu operatorów kluczowych jest uzależnione od:
  - kryteriów (określonych w ustawie w ślad za dyrektywą NIS)
  - progów istotności skutku zakłócającego usługę (określonych w rozporządzeniu)

NASK

Dziękuję za uwagę

Krzysztof.Silicki@nask.pl

NASK


ul. Kolska 12
01-045 Warszawa

tel.: +48 22 380 82 00
fax: +48 22 380 82 01

nask@nask.pl