Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

„Cyberbezpieczne wodociągi”

Wsparcie cyberbezpieczeństwa podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę

Marek Śliwiński

25.06.2025 r.

Informacje wstępne

Celem spotkania jest:

- przybliżenie wszystkim zainteresowanym podmiotom wstępnych założeń konkursu, co ułatwi przygotowanie się do wnioskowania o wsparcie w momencie rozpoczęcia naboru;
- omówienie przebiegu planowanego naboru wniosków o granty w tym: zakresu możliwego wsparcia, procesu oceny oraz pozostałych kwestii formalnych.

<u>UWAGA: Treść prezentacji zawiera informacje wstępne które mogą ulec zmianie</u>.
Dokumentem regulującym warunki udziału w konkursie będzie regulamin konkursu grantowego który zostanie opublikowany w momencie ogłoszenia konkursu.
Planowany termin naboru: sierpień 2025 r.
Ogłoszenie naboru nastąpi na stronie www Centrum Projektów Polska Cyfrowa: https://www.gov.pl/web/cppc/cppc-nabory

Powody uruchomienia wsparcia

„Wzmożona aktywność rosyjskich hakerów wymierzona w m.in. wodociągi i kanalizację (…) z 18 takich prób 17 zostało odpartych" - Minister Cyfryzacji

Wśród zaatakowanych obiektów znalazły się m.in.:

- Oczyszczalnia ścieków w Wydminach (kwiecień 2024)
- Oczyszczalnia ścieków w Kuźnicy (październik 2024)
- Stacje uzdatniania wody w Tolkmicku, Małdytach i Sierakowie (luty 2025)

W niektórych przypadkach cyberprzestępcy manipulowali parametrami urządzeń, ustawiając je na maksymalne wartości, co mogło prowadzić do poważnych zakłóceń w działaniu systemów.

Komunikat **Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT) z dnia 24.02.2025 r.**
https://www.gov.pl/web/baza-wiedzy/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-ws-atakow-na-przemyslowe-systemy-sterowania

Powody uruchomienia wsparcia

Tabela 1. Zestawienie liczby zarejestrowanych incydentów

CSIRT poziomu krajowego:	2023 r.	2024 r.	Zmiana procentowa:.
CSIRT NASK	80 267	103 449	+29%
CSIRT GOV	4 676	3 991	-15%
CSIRT MON	5 841	4 220	-28%
Sumaryczna roczna liczba zarejestrowanych incydentów:	90 784	111 660	**+23%**

Krajobraz Cyberprzestrzeni - **Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2024 rok**
https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie

Dyrektywa NIS2

Projekt ustawy o zmianie **ustawy o krajowym systemie cyberbezpieczeństwa** m.in. wdraża **Dyrektywę NIS2** (UC32: https://legislacja.gov.pl/projekt/12384504)

Rozszerzenie krajowego systemu cyberbezpieczeństwa do 18 sektorów gospodarki (ok. 10 tys. przedsiębiorców)

Wprowadzenie nowych obowiązków dla podmiotów kluczowych i ważnych

Podstawowy obowiązek to stosowanie odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu.

Wprowadzenie rozbudowanych środków nadzoru i egzekwowania przepisów

Założenia konkursu grantowego

CEL - Wsparcie podmiotów prowadzących działalność w zakresie zbiorowego zaopatrzenia w wodę, objętych krajowym systemem cyberbezpieczeństwa, wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS) w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa

ALOKACJA – ponad **300 mln zł** (netto), dofinansowanie 100% (brak wkładu własnego), VAT to wydatek niekwalifikowalny, dofinansowanie tylko na wydatki w kwocie netto.

ŹRÓDŁO FINANSOWANIA – Inwestycja C3.1.1. Krajowego Planu Odbudowy i Zwiększania Odporności (KPO)

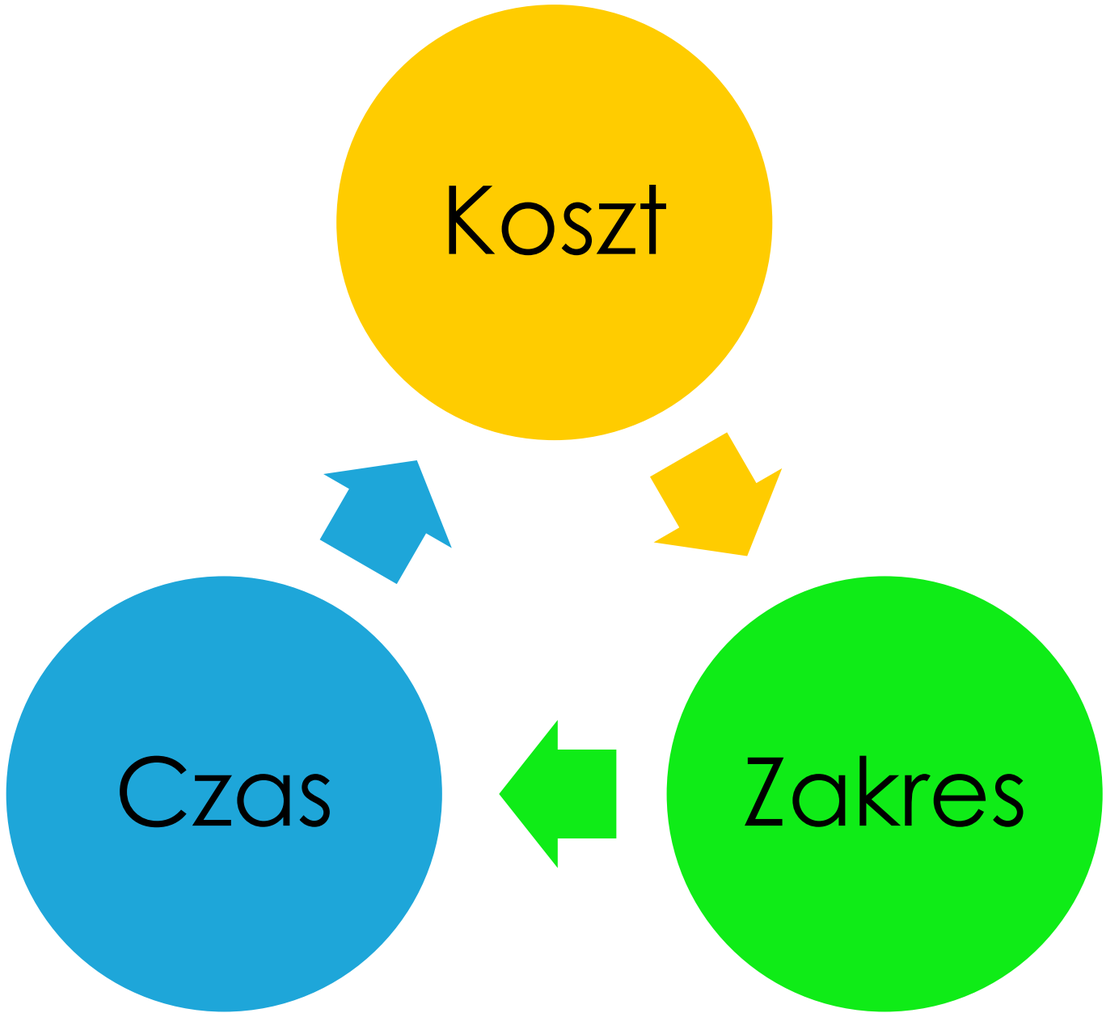
KRAJOWY PLAN ODBUDOWY

Rzeczpospolita Polska

Sfinansowane przez Unię Europejską NextGenerationEU

Ministerstwo Cyfryzacji

Założenia konkursu grantowego



Maksymalna wartość grantu to limit dostępnej pomocy de minimis tj. **maksymalnie 300 tys. EUR** (indywidualny limit można sprawdzić na stronie: https://sudop.uokik.gov.pl/ (istotny kurs PLN/EUR)

Możliwość kwalifikowania wydatków w okresie: od **1 stycznia 2025 r.** do **30 czerwca 2026 r.**

Wsparcie na wzmocnienie co najmniej jednego z trzech nw. obszarów cyberbezpieczeństwa:

- **Organizacyjny**
- **Techniczny (OT i IT)**
- **Kompetencyjny**

Obszary cyberbezpieczeństwa

Organizacyjny – wszelkie aspekty organizacyjne bezpieczeństwa systemów teleinformatycznych IT i OT, tj. audyt bezpieczeństwa, audyt zgodności z przepisami i normami, opracowanie, wdrożenie, utrzymanie i aktualizacja systemu zarządzania bezpieczeństwem informacji, systemu zarządzania bezpieczeństwem systemu teleinformatycznego IT/OT, systemu zarządzania ciągłością działania systemu teleinformatycznego IT/OT;

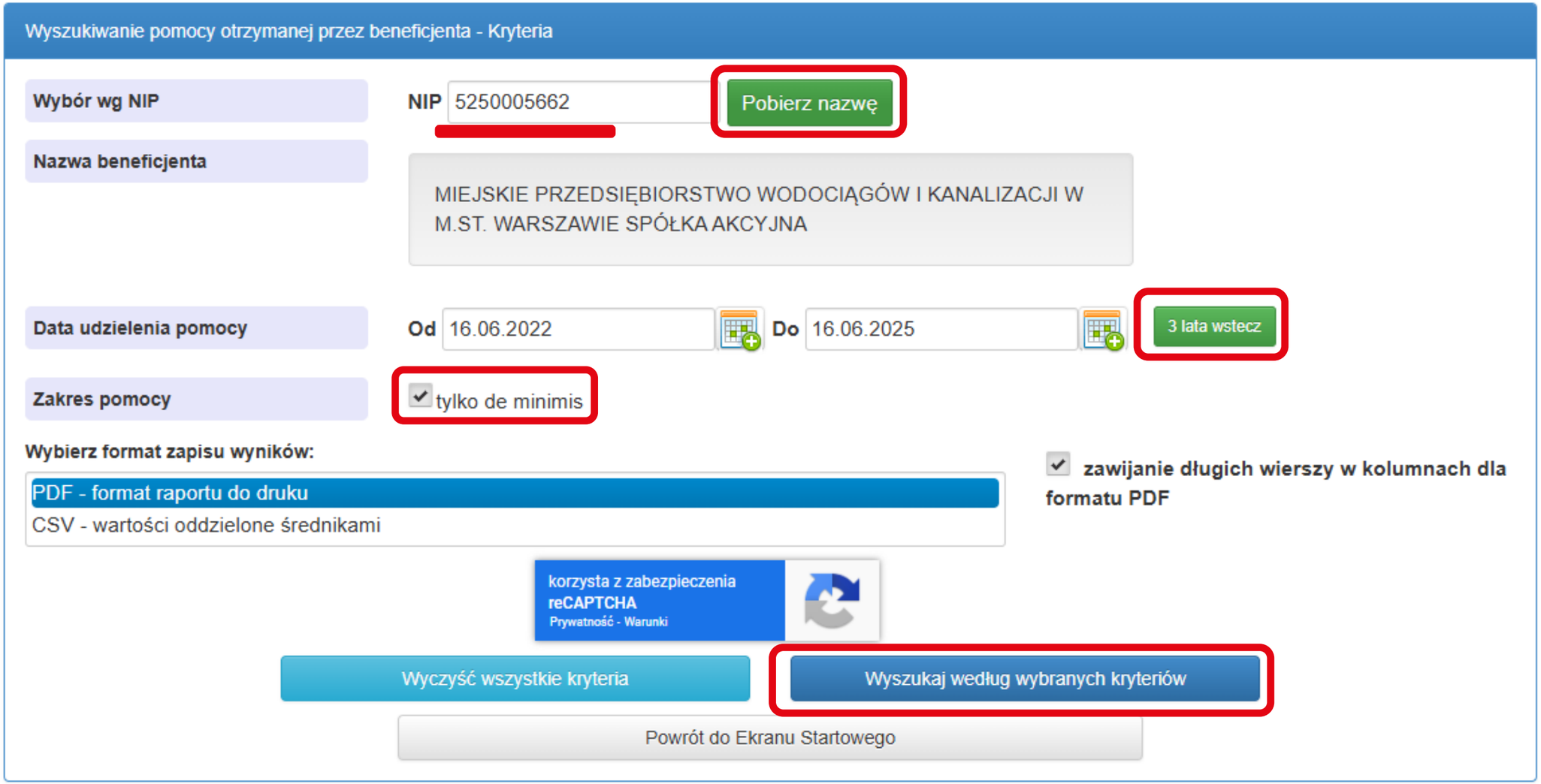
Kompetencyjny – wszelkie działania podnoszące świadomość, wiedzę i umiejętności na poziomie podstawowym, kierowniczym i specjalistycznym w zakresie cyberbezpieczeństwa, realizowane dla pracowników podmiotu, operatorów i administratorów systemów teleinformatycznych IT/OT, kadry kierowniczej IT/OT, kadry kierowniczej i zarządzającej podmiotu;

Obszary cyberbezpieczeństwa

Techniczny IT – dotyczy obszaru funkcjonalnego IT, obejmuje wszelkie komputerowe środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa komponentów środowiska teleinformatycznego IT, tj.: stacje robocze, serwery, dane biznesowe, oprogramowanie biznesowe, systemy pamięci masowej, urządzenia sieciowe i środowisko sieciowe, systemy bezpieczeństwa fizycznego i technicznego działające w sieci;

Techniczny OT – dotyczy obszaru funkcjonalnego OT (technologie operacyjne), obejmuje wszelkie komputerowe środki techniczne i wybrane elektrotechniczne środki techniczne – sprzętowe i aplikacyjne – służące do zabezpieczenia i zapewnienia bezpieczeństwa komponentów środowiska teleinformatycznego OT/ICS/IoT i środowiska IT obszaru przemysłowego OT, tj.: stacje robocze, serwery, dane systemów OT, systemy OT, oprogramowanie OT, urządzenia sieciowe i środowisko sieciowe OT, systemy bezpieczeństwa wizyjnego, fizycznego i technicznego w ramach infrastruktury wodociągowej (np. stacji uzdatniania wody, punktów poboru wody itp.) działające w sieci;

Jak określić mój limit? https://sudop.uokik.gov.pl/



https://sudop.uokik.gov.pl/

LISTA PRZYPADKÓW POMOCY DE MINIMIS OTRZYMANEJ PRZEZ BENEFICJENTA

Nazwa beneficjenta pomocy: MIEJSKIE PRZEDSIĘBIORSTWO WODOCIĄGÓW I KANALIZACJI W M.ST. WARSZAWIE SPÓŁKA AKCYJNA Zakres: od 16.06.2022 do 16.06.2025
Numer Identyfikacji Podatkowej (NIP) beneficjenta pomocy: 5250005662 Data wygenerowania: 16.06.2025

Lp.	Podstawa prawna - informacje podstawowe			Podstawa prawna - informacje szczegółowe			Numer środka pomocowego	Dzień udzielenia pomocy	Nazwa podmiotu udzielającego pomocy	NIP podmiotu udzielającego pomocy	Wartość nominalna pomocy [PLN]	Wartość pomocy brutto [PLN]	Wartość pomocy brutto [EURO]	Forma pomocy	Przeznaczenie pomocy
1	ustawa z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami		art. 81 ust. 1	brak	brak	W/UMWM-UU/UM/KP/7350/2022		28.11.2022	Marszałek Województwa Mazowieckiego	1132453940	138 515,40	138 515,4	29 575,19	otacja lub inne ezzwrotne wiadczenie	pomoc de minimis (zgodna z rozporządzeniem KE nr 1407/2013 lub wcześniejszym)
2	inne ustawy	USTAWA Z DNIA 19 LIPCA 2019 R. O ZAPEWNIENIU DOSTĘPNOŚCI OSOBOM ZE SZCZEGÓLNYMI POTRZEBAMI (DZ.U. Z 2022 R. POZ. 2240)	ART. 39 UST. 4			TARR-25/4/OP/FD/TARR/I/2024		29.03.2024	TARNOWSKA AGENCJA ROZWOJU REGIONALNEGO S.A.	8731013754	676 522,00	373 613,5	86 868,69	ożyczka referencyjna	pomoc de minimis (zgodna z rozporządzeniem KE nr 2023/2831)
3	ustawa z dnia 20 kwietnia 2004 r. o promocji zatrudnienia i instytucjach rynku pracy		Art. 69b	brak		12646.415.2024.RP		15.10.2024	Prezydent Miasta Stołecznego Warszawy	5252248481	47 457,36	47 457,3	11 058,97	otacja lub inne ezzwrotne wiadczenie	pomoc de minimis (zgodna z rozporządzeniem KE 2023/2831)
4	ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami		198l, 69a			Rep. A nr 5345/2025		07.04.2025	Starosta Powiatu Pruszkowskiego	5342405501	724 416,00	724 416,0	168 566,84	dotacja lub i bezzwrotne wiadczenie	pomoc de minimis stanowiąca rekompensatę za realizację usług świadczonych w ogólnym interesie gospodarczym (zgodna z rozporządzeniem KE 2023/2832)
Podsumowanie - łączna wartość pomocy udzielonej beneficjentowi:											1 586 910,76	1 284 002,33			

97 927,66

Ministerstwo Cyfryzacji

https://sudop.uokik.gov.pl/

https://uokik.gov.pl/public/zasady-pomocy-de-minimis

Podmiot, który otrzymał pomoc *de minimis* (stanowiącą rekompensatę za realizację usług świadczonych w ogólnym interesie gospodarczym) w rozumieniu rozporządzenia 2023/2832 w pełnej wysokości 750 000 EUR w ciągu 3 lat **może wciąż uzyskać pomoc *de minimis*** w rozumieniu rozporządzenia **2023/2831w pełnej wysokości 300 000 EUR** w ciągu 3 lat (**obie pomoce *de minimis* można ze sobą łączyć**)

Przeznaczenie pomocy
pomoc de minimis (zgodna z rozporządzeniem KE nr 1407/2013 lub wcześniejszym)
pomoc de minimis (zgodna z rozporządzeniem KE 2023/2831)
pomoc de minimis stanowiąca rekompensatę za realizację usług świadczonych w ogólnym interesie gospodarczym (zgodna z rozporządzeniem KE 2023/2832)

Kto może złożyć wniosek

Wsparcie może zostać udzielone podmiotowi prowadzącemu działalność w zakresie **zbiorowego zaopatrzenia w wodę**, objętemu krajowym system cyberbezpieczeństwa, wykorzystującemu technologie operacyjne w przemysłowych systemach sterowania, który jest:

- **przedsiębiorstwem wodociągowo-kanalizacyjnym, które jest operatorem usług kluczowych** w rozumieniu art. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), lub
- **spółką prawa handlowego** wykonującą zadania o charakterze użyteczności publicznej w rozumieniu przepisów ustawy z dnia 20 grudnia 1996 r. o **gospodarce komunalnej** (Dz. U. z 2021 r. poz. 679), lub
- **jednostką sektora finansów publicznych** w rozumieniu art. 9 pkt 2–4 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2024 r. poz. 1530, 1572, 1717, 1756, i 1907 oraz z 2025 r. poz. 39) – (**jednostki samorządu terytorialnego** oraz ich związki, samorządowe zakłady budżetowe)

Zakres wsparcia – wstępne założenia

Wsparcie może zostać udzielone **podmiotowi prowadzącemu działalność w zakresie zbiorowego zaopatrzenia w wodę**, na projekt grantowy, które realizuje co najmniej jeden z następujących celów z zakresu cyberbezpieczeństwa tego podmiotu:

- wdrożenie środków organizacyjnych służących zapewnieniu cyberbezpieczeństwa (**procedury i audyty**)
- zakup lub modernizację środków technicznych służących zapewnieniu cyberbezpieczeństwa (**sprzęt i usługi** – dotyczy IT jak i OT)
- rozwój kompetencji personelu w zakresie cyberbezpieczeństwa (**szkolenia**)

Możliwe będzie zabezpieczenie <u>całego</u> przedsiębiorstwa w zakresie IT, a w zakresie OT – instalacji dot. poboru, uzdatniania i dystrybucji wody.

Dobór działań niezbędnych do przeprowadzenia uzależniony będzie od indywidualnych potrzeb wnioskodawców

Wydatki kwalifikowalne i niekwalifikowalne

Szczegółowy katalog **wydatków kwalifikowalnych oraz niekwalifikowalnych** zostanie opublikowany w regulaminie konkursu grantowego (na stronie naboru). Na dzień organizacji webinaru(25.06.2025) niedostępny.

Katalog zostanie dostosowany do specyfiki branży m.in. katalog wydatków uwzględni wydatki obejmujące zabezpieczenie technologii OT. Przewidujemy wprowadzenie kategorii limitowanej dot. wsparcia zapewnienia ciągłości działania np. dotyczy zasilania awaryjnego

Przykład sposobu opisu wydatków kwalifikowalnych i niekwalifikowalnych zawarty w regulaminie konkursu „**Cyberbezpieczny Rząd**”
https://www.gov.pl/web/cppc/inwestycja-c-311-konkurs-grantowy-cyberbezpieczny-rzad

Kategorie wydatków kwalifikowalnych

- **środki trwałe/dostawy** (np. sprzęt informatyczny i urządzenia bezpieczeństwa)

- **wartości niematerialne i prawne**, w szczególności autorskie prawa majątkowe lub licencje, w tym subskrypcyjne, na korzystanie z oprogramowania, w tym systemowego o przewidywanym okresie używania dłuższym niż rok, prawa do dokumentacji, raportów i opracowań

- **usługi zewnętrzne,** w szczególności merytoryczne przygotowanie projektu grantowego przez osoby lub podmioty zewnętrzne, usługi informatyczne i szkolenia zwiększające poziom bezpieczeństwa informacji, usługi wspomagające realizację projektu grantowego, w szczególności usługi doradcze osób lub podmiotów zewnętrznych oraz szkolenia, audyty oraz wdrożenie zarządzania bezpieczeństwem i ciągłością działania systemów teleinformatycznych IT/OT

- **koszty pośrednie (<u>kwota ryczałtowa do 5% wartości grantu</u>)**, w szczególności możliwość rozliczenia m.in. kosztów administracyjnych, delegacji, wynagrodzenia kadry zarządzającej projektem grantowym oraz wynagrodzeń osób (umów o pracę) zatrudnionych u grantobiorcy i bezpośrednio zaangażowanych w projekt grantowy (m.in. inżynier kontraktu, ekspert z dziedziny cyberbezpieczeństwa)

Ograniczenia dot. wydatków

Kwalifikowalne będą tylko koszty poniesione **w okresie realizacji przedsięwzięcia** grantowego. Koszty usług np. gwarancji, licencji, ubezpieczenia wykraczające poza okres kwalifikowalności będą kwalifikowalne proporcjonalnie w czasie trwania okresu kwalifikowalności (+ obowiązek zapewnienia trwałości wdrażanych rozwiązań).

Łącznie **do 20% wydatków kwalifikowalnych projektu** grantowego może zostać poniesione na wydatki które mają wpływ na zapewnienie **ciągłości działania systemów teleinformatycznych OT np.:**

- Zasilanie awaryjne: generatory prądu i ups do serwerów, baterie do ups.
- Zabezpieczenie systemów bezpieczeństwa: wizyjnego, dostępu fizycznego i zabezpieczeń technicznych infrastruktury wodociągowej np. stacji uzdatniania wody, punktów poboru wody - działających w sieci rozległej.

Przykłady dofinansowanych rozwiązań

Obszar	Rozwiązanie obszarowe bezpieczeństwa	Przykłady rozwiązań
Organizacyjny	1.1 Systemowe zarządzanie bezpieczeństwem i ciągłością działania IT/OT	Opracowanie, wdrożenie, przegląd i aktualizacja dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), audyt SZBI, Systemu Zarządzania Ciągłością Działania STI (SZCD STI), audyt SZCD STI, audyt zgodności z KRI/uoKSC, (re)certyfikacja SZBI, SZCD na zgodność z normami, utrzymanie i zarządzanie SZBI, SZCD
Kompetencyjny	2.1 Szkolenia z zakresu cyberbezpieczeństwa *(kolorem oznaczone rozwiązania premiowane)*	Podstawowe szkolenia (lub dostęp do platform szkoleniowych) budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników, szkolenia z zakresu cyberbezpieczeństwa dla kadr istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji, szkolenia specjalistyczne dla kadry zarządzającej i informatyków w zakresie zastosowanych lub planowanych do zastosowania środków bezpieczeństwa w ramach projektu, szkolenia powiązane z testami socjotechnicznymi, które będą weryfikować świadomość zagrożeń i reakcji personelu, w szczególności reagowanie specjalistów posiadających odpowiednie obowiązki w ramach SZBI w zgodzie z przyjętymi procedurami, usługi typu security awareness do symulowanych ataków socjotechnicznych, szkolenia przygotowujące do certyfikacji z zakresu cyberbezpieczeństwa

Przykłady dofinansowanych rozwiązań

Obszar	Rozwiązanie obszarowe bezpieczeństwa	Przykłady rozwiązań
Techniczny IT	3.1 Bezpieczeństwo systemów informatycznych	Testy bezpieczeństwa, usługa skanowania podatności, skaner podatności, system klasy BAS (Breach and attack simulation), oprogramowanie do badania podatności w kodzie aplikacji, oprogramowanie antywirusowe, EDR, XDR, ITDR, NDR
	3.2 Bezpieczeństwo www (stron i/lub platform internetowych)	Oprogramowanie do zarządzania podatnościami, WAF, Firewall, NGFW, UTM
	3.3 Bezpieczeństwo stacji roboczych	Oprogramowanie antywirusowe, EDR, XDR, ITDR
	3.4 Rozwiązanie bezpieczeństwa sieci	UTM, NGFW, IPS/IDS, Firewall, oprogramowanie antywirusowe, SASE VPN, VPN, NAC, EDR, XDR, NDR, Network Security Policy Management & Orchestration
	3.5 Rozwiązania bezpieczeństwa styku sieci internet z usługami wewnętrznymi	WAF, NGFW, IPS/IDS, Proxy Serwer , oprogramowanie antywirusowe, HoneyPot, Web Secure Gateway , Email Secure Gateway, urządzenia i oprogramowanie typu Sandbox
	3.6 Zwiększenie niezawodności i wydajności	SAN, NAS, rozbudowa pamięci RAM, dyski twarde (HDD, SDD, funkcjonalność hot swap), macierz dyskowa, rozwiązanie RAID, rozbudowa serwera o dodatkowy procesor, serwer pod rozwiązania bezpieczeństwa

Przykłady dofinansowanych rozwiązań

Obszar	Rozwiązanie obszarowe bezpieczeństwa	Przykłady rozwiązań
Techniczny IT	3.6 Rozwiązania sieciowe WAN/LAN/WIFI	Zarządzalny switch z obsługą VLAN, MACsec, standard 802.1X, zarzadzalne centralne urządzenie WiFi, Acces Point WiFi, NAC
	3.7 Rozwiązania wirtualizacyjne	System wirtualizacji, serwer do systemu wirtualizacji
	3.8 Rozwiązania kopii zapasowych	Deduplikator, serwer kopii zapasowych, streamer, kaseta do Streamera, NAS, usługa kopii zapasowych w chmurze obliczeniowej
	3.9 Redundancja (HA)	Rozwiązanie RAID, serwer w HA, NAS w HA, SAN, zarządzalne urządzenia sieciowe w HA, usługa redundancji w chmurze obliczeniowej
	3.10 Rozwiązania zarządzania operacyjnego	ITSM, oprogramowanie do monitorowania infrastruktury informatycznej, oprogramowanie do zarządzania i aktualizacji systemów operacyjnych i oprogramowania na stacjach roboczych, serwerach, urządzeniach sieciowych, MDM, monitorowanie NetFlow
	3.11 Bezpieczeństwo komunikacji	Email Secure Gateway, Web Secure Gateway, EDR, XDR, Sandbox, oprogramowanie antywirusowe, certyfikaty SSL, HSM/Software HSM

Przykłady dofinansowanych rozwiązań

Obszar	Rozwiązanie obszarowe bezpieczeństwa	Przykłady rozwiązań
Techniczny IT	3.12 Monitorowanie bezpieczeństwa	EDR, XDR, NDR, ITDR, SIEM, SOAR, HoneyPot, menadżer logów, DLP, Network Security Policy Management & Orchestration, usługa typu MDR (Managed Detection and Response), usługa SOC (Security Operation Center), usługa CTI (Cyber Threat Intelligence)
	3.13 Reagowanie w zakresie bezpieczeństwa	EDR, XDR, NDR, ITDR, SOAR, AntyDDoS, Network Security Policy Management & Orchestration, usługa typu MDR (Managed Detection and Response)
	3.14 Zarządzanie uprawnieniami użytkowników	Oprogramowanie do zarządzania tożsamością i dostępem, IAM, PIM, PAM, centralny menedżer haseł, rozwiązanie MFA, klucze U2F, NAC
	3.15 Zabezpieczanie dowodów cyfrowych	Oprogramowanie do analizy powłamaniowej, urządzenia do analiz powłamaniowych, analiza i zabezpieczanie dowodów cyfrowych

Przykłady dofinansowanych rozwiązań

Obszar	Rozwiązanie obszarowe bezpieczeństwa	Przykłady rozwiązań
Techniczny OT	4.1 Bezpieczeństwo systemów sterowania przemysłowego (OT/ICS/IIoT) 4.2 Bezpieczeństwo stacji roboczych OT/ICS 4.3. Rozwiązania bezpieczeństwa sieci OT/ICS/IIoT 4.4 Rozwiązania sieciowe WAN/LAN/WiFi OT/ICS/IIoT 4.5 Rozwiązania bezpieczeństwa styku sieci internet z siecią OT/ICS/IIoT 4.6 Rozwiązania bezpieczeństwa styku sieci wewnętrznej IT z siecią OT/ICS/IIoT 4.7 Rozwiązania kopii zapasowych konfiguracji i danych systemów OT/ICS/IIoT 4.8 Redundancja (HA) OT/ICS/IIoT 4.9 Rozwiązania zarządzania operacyjnego infrastrukturą OT/ICS/IIoT 4.10 Monitorowanie bezpieczeństwa OT/ICS/IIoT 4.11 Reagowanie w zakresie bezpieczeństwa OT/ICS/IIoT	Firewall sieciowy z IPS dedykowany sieciom OT, NGFW (Next Gen FireWall) z IPS dedykowany sieciom OT, SIEM (Security Information and Event Management) OT, SOAR (Security Orchestration, Automation and Response) OT, HoneyPot, UTM (Unified Threat Management) z IPS dedykowany sieciom OT, licencje na IPS (Intrusion Prevention System) dedykowany sieciom OT, IDS (Intrusion Detection System) dedykowany sieciom OT, serwer fizyczny niezbędny do zainstalowania produktu lub wdrożenia rozwiązania z zakresu bezpieczeństwa, zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch), system monitorujący pracę urządzeń sieciowych OT/ICS/IoT, klucze sprzętowe U2F, szafa RACK do produktów i rozwiązań z zakresu bezpieczeństwa, bramy jednokierunkowe (Unidirectional Gateway / Data Diode), sprzętowe sondy/sensory do monitorowania sieci OT (dedykowane urządzenia do analizy protokołów przemysłowych), urządzenia do obsługi sieci Private APN, łączność przewodowa z zasilaniem w sieci OT, system klasy PAM, stacja robocza fizyczna lub wirtualna z rolą stacji przesiadkowej dedykowany do rozwiązań OT, infrastruktura PKI wraz z niezbędnymi elementami, urządzenia sieciowe z obsługą urządzeń OT/ICS/IoT

Przykłady dofinansowanych rozwiązań

Obszar	Rozwiązanie	Przykłady rozwiązań
Techniczny OT	4.12 Wsparcie ciągłości działania infrastruktury obszaru OT (techn. IT/OT/ICS/IIoT) (**wydatki limitowane 20%**)	Urządzenia typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa, akumulatory do urządzeń typu UPS do produktów i rozwiązań z zakresu bezpieczeństwa, agregat prądotwórczy, mobilny agregat prądotwórczy, przyłącze elektryczne do agregatów prądotwórczych, Firewall (NGFW), system ADDoS do zabezpieczenia systemów bezpieczeństwa: wizyjnego, dostępu fizycznego i zabezpieczeń technicznych infrastruktury wodociągowej np. stacji uzdatniania wody, punktów poboru wody - działających w sieci rozległej.

Wydatki niekwalifikowalne

Do wydatków niekwalifikowanych w ramach grantu zalicza się w szczególności wydatki na zakup, dostawę lub usługi, które **nie służą bezpośrednio wsparciu cyberbezpieczeństwa**, w szczególności:

- komputery stacjonarne i przenośne, urządzenia mobilne (smartfony, tablety)
- akcesoria i urządzenia peryferyjne (np. drukarki, skanery, urządzenia wielofunkcyjne, kserokopiarki)
- oprogramowanie biurowe, oprogramowanie do elektronicznego zarządzania dokumentacją i oprogramowanie systemów operacyjnych
- szkolenia niezwiązane z cyberbezpieczeństwem
- usługi dostępu do internetu, abonamenty telefoniczne
- budowa infrastruktury sieci LAN/WAN/radiowej/światłowodowej
- budowa infrastruktury systemów bezpieczeństwa: wizyjnego, dostępu fizycznego i zabezpieczeń technicznych
- podatek VAT oraz wynagrodzenia pracowników jako koszty bezpośrednie

Ramowe zasady oceny wniosków

Wnioski złożone na konkurs podlegać będą ocenie formalnej i ocenie merytorycznej. Czas na uzupełnienia wniosku w terminie nie krótszym niż 7 dni roboczych od dnia wysłania wezwania do uzupełnienia wniosku (§ 10 ust.6 rozporządzenia de minimis)

Projekty które spełnią wszystkie wymagania niezbędne (ocenione pozytywnie), zostaną ujęte na liście rankingowej. Kolejność na liście rankingowej uzależniona będzie od:
1) **oceny deklarowanego przyrostu odporności** na cyberzagrożenia w zakresie poszczególnych **rozwiązań obszarowych bezpieczeństwa** (slajdy 18-23)**. Im większa liczba uzyskanych punktów, tym wyższa ocena.** Skala oceny od 0 do 3 pkt. za każde rozwiązanie w którym planowane będą działania (0 - brak rozwiązania, 1 – niski, 2 – średni, 3 - wysoki).
2) w przypadku, gdy co najmniej dwa wnioski uzyskają **taką samą liczbę punktów** na liście rankingowej, a pozostałe do rozdysponowania **środki będą niewystarczające** dla objęcia wsparciem każdego z tych projektów grantowych w pełnej wysokości, grant otrzyma ten Wnioskodawca grantu, **który złożył wniosek wcześniej.**

Ramowe zasady oceny wniosków

Premiowane będą działania podnoszące w największym stopniu odporność na cyberzagrożenia (rozwiązania oznaczone kolorem zielonym). W szczególności rozwiązania w których wykorzystywane są technologie operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS). Premia oznacza przyznanie dodatkowych punktów (bonus) za wzrost odporności w premiowanych rozwiązaniach bezpieczeństwa.

Dofinansowanie otrzymają projekty w ramach limitów obejmujących:

1) Wartość alokacji (do wyczerpania środków)
2) Docelowy poziom wskaźnika obowiązującego dla Inwestycji C.3.1.1 KPO tj. objęcia wsparciem 500 podmiotów KSC.
   „*Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS)*”

Wymagane załączniki

- **Oświadczenie** o nieotrzymaniu pomocy de minimis lub **zaświadczenia** o otrzymanej pomocy de minimis (SKAN) (potwierdzenie wykorzystanego limitu pomocy 300 tys.euro)
- **Formularz** informacji przedstawianych przy ubieganiu się o pomoc de minimis (art. 37 ust. 1 pkt 2 ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej)

- **Zezwolenie** na prowadzenie zbiorowego zaopatrzenia w wodę, o którym mowa w art. 16 ust. 1 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, **albo oświadczenie**, że podmiot prowadzący działalność w zakresie zbiorowego zaopatrzenia w wodę, objęty krajowym system cyberbezpieczeństwa, przedsiębiorstwo wodociągowo-kanalizacyjne jest podmiotem, o którym mowa w art. 16 ust. 3 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu

- **Oświadczenie** o zapoznaniu się i deklaracja implementacji wytycznych Komunikatu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT)

Ramowy harmonogram konkursu grantowego

Etapy konkursu grantowego Cyberbezpieczne Wodociągi	2025 r.					2026 r.					
	VIII	IX	X	XI	XII	I	II	III	IV	V	VI
Ogłoszenie naboru wniosków do konkursu grantowego											
Nabór wniosków o grant											
Ocena wniosków											
Ogłoszenie listy rankingowej wniosków objętych wsparciem											
Zawieranie umów z grantobiorcami											
Przekazanie środków grantobiorcom (jedna transza)											
Realizacja projektów grantowych (**kwalifikowalność wydatków od 1.01.2025 r. do 30.06.2026 r.**)											
Złożenie wniosku rozliczającego (**do 30.06.2026 r.**)											

Jak przygotować się do naboru?

Każdy wnioskodawca określa indywidualny limit (jeśli korzystał w ciągu 3 lat z pomocy de minimis) – nie można przekroczyć 300 tys. Euro na 3 lata (sprawdzamy dane na stronie: https://sudop.uokik.gov.pl/)

Zapoznać się z komunikatem Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w sprawie ataków na przemysłowe systemy sterowania (ICS/OT) i ocenić potrzeby finansowe dotyczące wdrożenia niezbędnych zmian w zakresie bezpieczeństwa

Zdefiniować zakres priorytetowych potrzeb (np. szkolenia, sprzęt, doradztwo, licencje itp.) Zebrać oferty, wycenić zakres usług i czas niezbędny na przeprowadzenie wdrożenia (rozwiązania muszą zostać wdrożone w organizacji w krótkim czasie)

Zbudować zespół projektowy, który przygotuje i przeprowadzi projekt. Jeśli brakuje specjalistycznej wiedzy, pozyskać do współpracy podmiot z rynku który będzie wspierał i doradzał

Po opublikowaniu regulaminu przeczytać dokładnie dokumentację + wzór umowy: m.in. **3-letni obowiązek zachowania trwałości wdrażanych rozwiązań.**

Zapoznać się z rozporządzeniem ws. udzielania pomocy ***de minimis*** *(obowiązuje)* https://dziennikustaw.gov.pl/DU/2025/729

Przewidywany **termin uruchomienia konkursu** – **SIERPIEŃ 2025** (I-sza połowa miesiąca) – nabór wniosków potrwa **min. 30 dni**.

Nabór grantów prowadzić będzie **Centrum Projektów Polska Cyfrowa** https://www.gov.pl/web/cppc/cppc-nabory

W planie uruchomienie dedykowanej **infolinii** i **HelpDesku** dla wnioskodawców – przed uruchomieniem naboru. **Kolejny webinar** – kilka dni po starcie naboru wniosków. Adres @ dedykowany do konkursu: **cyberbezpiecznewodociagi@cppc.gov.pl**

Komunikaty o projekcie na stronie Ministerstwa Cyfryzacji - https://www.gov.pl/web/baza-wiedzy/aktualnosci

Ministerstwo Cyfryzacji

Dziękuję za uwagę