NAJWYŻSZA IZBA KONTROLI

Departament Administracji Publicznej

KAP.410.2.5.2025

Pan Wojciech Szajnar
Dyrektor Centrum Projektów
Polska Cyfrowa

ul. Spokojna 13a
01–044 Warszawa

WYSTĄPIENIE POKONTROLNE

P/25/003 Realizacja projektu Cyberbezpieczny Samorząd

NAJWYŻSZA IZBA KONTROLI
Departament Administracji Publicznej
ul. Filtrowa 57, 02-056 Warszawa
tel. 48224445308, kap@nik.gov.pl

I. Dane identyfikacyjne

Jednostka kontrolowana	Centrum Projektów Polska Cyfrowa[1], ul. Spokojna 13a, 01-044 Warszawa
Kierownik jednostki kontrolowanej	Wojciech Szajnar, Dyrektor Centrum Projektów Polska Cyfrowa, od 18 lipca 2018 r.
Zakres przedmiotowy kontroli	Realizacja przez Centrum Projektów Polska Cyfrowa projektu grantowego „Cyberbezpieczny Samorząd”
Okres objęty kontrolą	Od 1 stycznia 2023 r. do dnia zakończenia czynności kontrolnych w 2025 r., tj. do 5 września 2025 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[2]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Administracji Publicznej
Kontrolerzy	Tomasz Kwitowski, doradca techniczny, upoważnienie do kontroli nr KAP/57/2025 z 12 maja 2025 r. Ewa Bimkiewicz, specjalista kontroli państwowej, upoważnienie do kontroli nr KAP/58/2025 z 12 maja 2025 r.

(akta kontroli str. 1-4)

[1] Dalej: CPPC, Beneficjent lub Partner Wiodący.

[2] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[3] kontrolowanej działalności

OCENA OGÓLNA

W CPPC zorganizowano konkurs grantowy w ramach projektu „Cyberbezpieczny Samorząd”[4] (dalej: Projekt) zgodnie z obowiązującymi regulacjami. Zawarto 2497 umów o powierzeniu grantów ze wszystkimi zainteresowanymi jednostkami samorządu terytorialnego (dalej: JST), których wnioski spełniały warunki przyznania dofinansowania w ramach Projektu, a także monitorowano realizację Projektu. Nieprawidłowości stwierdzone w działalności CPPC jako Beneficjenta Projektu nie miały dotychczas zasadniczego wpływu na realizację Projektu. Wskaźniki w ramach Projektu nie mierzyły bezpośrednio w jakim stopniu realizacja umów grantowych przyczyni się do osiągnięcia celu Projektu założonego we Wniosku o dofinansowanie[5], tj. zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych JST. Przyjęto, że zrealizowanie umów o powierzeniu grantów przyczyni się do podniesienia poziomu bezpieczeństwa informacji JST.

Uzasadnienie oceny ogólnej

CPPC prawidłowo zorganizowało nabór wniosków do Konkursu Grantowego pn. „Cyberbezpieczny Samorząd” (dalej: konkurs grantowy), określiło kryteria wyboru projektów i zapewniło JST równy dostęp do środków grantowych. Ustanowiono struktury zarządcze, w tym wyznaczono pracowników odpowiedzialnych za realizację Projektu. Określono system monitorowania wskaźników produktu i rezultatu dla Projektu. W ramach systemu monitorowania organizowano cotygodniowe spotkania z przedstawicielami Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (dalej: NASK lub Partner Projektu), podczas których omawiano bieżące tematy związane z realizacją Projektu, postępy prac, trudności i ryzyka. Analizowano raporty Partnera z realizacji Projektu w zakresie liczby podpisanych umów, zleconych i wypłaconych przelewów, złożonych wniosków o kolejne transze, wniosków końcowych i sprawozdań. W dokumentacji konkursu grantowego nie przewidziano oceny poziomu cyberbezpieczeństwa JST na etapie składania wniosków o grant oraz nie powiązano kwalifikowalności wydatków ponoszonych w ramach umów o powierzeniu grantów ze wzrostem poziomu cyberbezpieczeństwa JST po wykorzystaniu grantu.

W związku z realizacją Projektu przewidziano zarządzanie ryzykiem i zidentyfikowano 11 ryzyk, jednak w analizie ryzyka zamiast wymaganych mechanizmów kontrolnych opisano mechanizmy zapobiegania, które, zdaniem NIK, nie zapewniały bezzwłocznego podjęcia działań zaradczych w przypadku wystąpienia ryzyka, co było działaniem nierzetelnym i ogranicza skuteczność systemu zarządzania Projektem.

Przyjęty w Projekcie system monitorowania wskaźników nie dostarczał informacji na temat postępu rzeczowego, ponieważ CPPC dotychczas dokumentowało i sprawozdawało monitorowanie tylko jednego wskaźnika

---

[3] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[4] Projekt realizowany w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

[5] Nr FERC.02.02-IP.01-0001/23, dalej: WoD.

dotyczącego liczby podmiotów wspartych w zakresie cyberbezpieczeństwa, co było działaniem nierzetelnym.

W ramach Projektu CPPC dopuściło możliwość jednoczesnego funkcjonowania systemów dziedzinowych i bezpieczeństwa na serwerach nabywanych przez JST w ramach grantów na zwiększenie bezpieczeństwa informacji, co było niezgodne z wymogami § 15 pkt 1 rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[6] (dalej: KRI).

Ponadto stwierdzono nieprawidłowości polegające m.in. na:

- poniesieniu przez CPPC jako Beneficjenta w ramach zadania nr 5 „Ewaluacja, rozliczenie projektu" wydatków w wysokości 828,3 tys. zł przed planowanym terminem jego rozpoczęcia, co było niezgodne z postanowieniami § 5 ust. 8 Decyzji o dofinansowaniu projektu „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (dalej: DoD), a także z § 4 ust. 3 Umowy o partnerstwie w celu wspólnej realizacji projektu pn. „Cyberbezpieczny Samorząd" w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 z 14 lipca 2023 r. (dalej: UoP);
- niewystąpieniu Beneficjenta do Instytucji Pośredniczącej[7] (dalej: IP) w sprawie potrzeby zmiany wskaźników w związku z brakiem możliwości osiągnięcia dwóch zaplanowanych wskaźników w ramach Projektu, co było nierzetelne.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[8] kontrolowanej działalności

OBSZAR

Realizacja przez Centrum Projektów Polska Cyfrowa Projektu Grantowego „Cyberbezpieczny Samorząd"

Opis stanu faktycznego

1. Decyzją Zastępcy Dyrektora CPPC[9] ustanowiono strukturę zarządczą Projektu, która podlegała zmianom w zależności od etapu przedsięwzięcia i zachodzących

---

6 Dz.U. poz. 773.

7 CPPC pełni rolę zarówno Beneficjenta, jak i Instytucji Pośredniczącej w Programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

8 Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

9 Decyzja nr 5/2023 Zastępcy Dyrektora Centrum Projektów Polska Cyfrowa z dnia 28 lipca 2023 r. w sprawie powołania Zespołu ds. realizacji projektu pozakonkursowego CPPC (beneficjenta projektu) nr FERC.02.02-IP.01-0001/23 pn. „Cyberbezpieczny Samorząd", zmieniona decyzją nr 2/2024 Zastępcy Dyrektora Centrum Projektów Polska Cyfrowa z dnia 26.02.2026 r. w sprawie powołania Zespołu ds. realizacji projektu pozakonkursowego CPPC (beneficjenta projektu) nr FERC.02.02-IP.01-0001/23 pn. „Cyberbezpieczny Samorząd, zmieniona decyzją nr 4/2024 Zastępcy Dyrektora Centrum Projektów Polska Cyfrowa z dnia 28.06.2024 r. w sprawie powołania Zespołu ds. realizacji projektu pozakonkursowego CPPC (beneficjenta projektu) nr FERC.02.02-IP.01-0001/23 pn. „Cyberbezpieczny Samorząd, zmieniona decyzją nr 3/2025 Zastępcy Dyrektora Centrum Projektów Polska Cyfrowa w sprawie powołania Zespołu ds. realizacji Projektu własnego nr FERC.02.02-IP.01-0001/23 pn. „Cyberbezpieczny Samorząd", zmieniona decyzją nr 10/2025 Zastępcy Dyrektora Centrum Projektów Polska Cyfrowa z dnia 9 maja 2025 r. w sprawie

zmian w zatrudnieniu. W okresie objętym kontrolą Zespół projektowy liczył 11 osób. Zarządzeniem Dyrektora CPPC[10] wprowadzono zasady rozdzielności funkcji odnośnie do projektów własnych, pomiędzy IP a Beneficjentem. Według tych zasad, do zadań Beneficjenta należy w szczególności: przygotowanie, podpisanie i złożenie wniosku o dofinansowanie, podpisanie umowy (w przypadku przedmiotowego projektu decyzji) o dofinansowanie, aneksów, utworzenie zespołu projektowego, realizacja projektu i poddanie się kontroli zgodnie z postanowieniami umowy (tu: decyzji) o dofinansowanie. W zasadach określono też, że zespół Beneficjenta stanowią pracownicy Biura Projektów Własnych lub Kierownik projektu oraz wskazani w decyzji o powołaniu zespołu projektowego pracownicy Komórek wspierających, a pracownicy IP nie biorą udziału w zadaniach wykonywanych przez zespół Beneficjenta. CPPC działające jako IP wykonuje swoje zadania zgodnie z dyspozycjami art. 9 ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027[11] (dalej: ustawa wdrożeniowa), z uwzględnieniem Porozumień oraz właściwych wytycznych i instrukcji wykonawczych obowiązujących w CPPC.

(akta kontroli: CD plik 003)

2. W 2023 r. w ramach konkursu grantowego zorganizowano nabór wniosków, w którym złożono 2614 wniosków na łączną kwotę 1 538 611,8 tys. zł. Ocenie poddano 2515 wniosków (316 w 2023 r. i 2199 w 2024 r.) o łącznej wartości 1 486 209,5 tys. zł. Wszystkie umowy o powierzenie grantu zawarto z JST w 2024 r. Było to 2497 umów na kwotę 1 475 253,3 tys. zł. Realizacja projektów rozpoczęła się w 2025 r. Na dzień 31 sierpnia 2025 r. realizowanych było 2490 projektów grantowych o łącznej wartości 1 471 218,6 tys. zł. Na dzień 31 sierpnia 2025 r. Grantobiorcy złożyli 26 wniosków o płatność rozliczających grant na kwotę 16 072,6 tys. zł, z których do dnia zakończenia kontroli NASK rozliczył 17 na kwotę 10 753,5 tys. zł. Na dzień 31 sierpnia 2025 r. kwota wykorzystana dla całego Projektu kształtuje się na poziomie 1 122 238,9 tys. zł, co stanowi 62,4% całkowitej alokacji.

W ramach Projektu zaplanowano jeden nabór grantowy. Tryb wyboru wniosków o dofinansowanie określono w jednym z elementów dokumentacji konkursu grantowego - *Schemacie grantowym* (dalej: Schemat), który został przekazany do IP przez Beneficjenta 18 lipca 2023 r., a zatem na dzień przed rozpoczęciem naboru grantowego. Ostatecznie dokumentacja konkursu grantowego wraz ze Schematem została zaakceptowana przez Instytucję Zarządzającą oraz IP w dniu 11 sierpnia 2023 r., a zatem 17 dni roboczych po terminie rozpoczęcia naboru. Mając na względzie ten termin, zakres zmian oraz jednoczesne przedłużenie

---

powołania Zespołu ds. realizacji Projektu własnego nr FERC.02.02-IP.01-0001/23 pn. „Cyberbezpieczny Samorząd".

[10] Zarządzenie nr 16/2022 Dyrektora Centrum Projektów Polska Cyfrowa z dnia 30 grudnia 2022 r. w sprawie wprowadzenia wytycznych w zakresie funkcjonowania Centrum Projektów Polska Cyfrowa w zakresie rozdzielności funkcji, zmienione zarządzeniem nr 2/2024 Dyrektora Centrum Projektów Polska Cyfrowa z 4 kwietnia 2024 r. w sprawie wprowadzenia zasad rozdzielności funkcji w Centrum Projektów Polska Cyfrowa, zmienione zarządzeniem nr 11/2024 Dyrektora Centrum Projektów Polska Cyfrowa z 27 września 2024 r. w sprawie wprowadzenia zasad rozdzielności funkcji w Centrum Projektów Polska Cyfrowa.

[11] Dz. U. poz. 1079, ze zm.

terminu składania wniosków o granty, NIK uznaje, że ogłoszenie konkursu z warunkowo zaakceptowaną dokumentacją naboru nie miało wpływu na przebieg konkursu. Zgodnie z treścią Schematu realizacja konkursu pn. „Cyberbezpieczny Samorząd" nastąpiła w formie projektu grantowego w rozumieniu art. 41 ustawy wdrożeniowej. Nabór, wraz ze wszystkimi dokumentami, ogłoszono na stronie internetowej: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (29.08.2025 r., godz. 13.54).

W ramach Projektu nie wyczerpano pełnej puli środków przewidzianej na jego realizację (alokacja wynosiła 1 874 294,0 tys. zł, w tym 1 494 000,0 tys. zł z budżetu środków europejskich i 380 294,3 tys. zł z budżetu państwa, a bez wkładu własnego Grantobiorców 1 798 235,4 tys. zł). Do 31 sierpnia 2025 r. kwota niewykorzystanych środków wynosiła 675 996,5 tys. zł (tj. 36,1%). Beneficjent rozwiązał siedem umów grantowych, wszystkie na wniosek Grantobiorców, na łączną kwotę 4 132,7 tys. zł. Z uwagi na to, że w konkursie grantowym wzięło udział 89% jednostek uprawnionych, Beneficjent nie badał powodów odstąpienia pozostałych JST od udziału w naborze. Beneficjent nie przewiduje dodatkowych naborów. Odnośnie powodów, dla których nie przewidziano dodatkowych naborów dyrektor CPPC wyjaśnił, że *decyzja o nieuruchamianiu kolejnych naborów została podjęta po analizie zainteresowania projektem, możliwości realizacyjnych jednostek samorządu terytorialnego (JST), oraz efektywności wykorzystania dostępnych środków. Należy zauważyć, że pomimo wydłużenia terminu trwania pierwotnego naboru, w dalszym ciągu nie wszystkie JST zdecydowały się na udział w nim. Samorządy, które były zdecydowane na udział, złożyły wnioski w wyznaczonym czasie. Grupa, która nie złożyła wniosków wynosiła około 10% wszystkich JST, co wskazuje na brak szerszego zapotrzebowania na dodatkowe nabory. Także wśród samorządów, które początkowo złożyły wnioski, występowały przypadki niepodpisania Umowy, lub zdecydowania się na jej rozwiązanie w trakcie realizacji. Analiza budżetu projektu w kontekście powstałych oszczędności wykazała, że ewentualny dodatkowy nabór mógłby być:*

- *ograniczony wyłącznie do JST, które nie złożyły wniosków wcześniej. Jednakże, jak wynika z dotychczasowych obserwacji, ta grupa nie wykazywała zainteresowania projektem,*
- *otwarty dla wszystkich JST (przy założeniu udziału ok. 2000–2500 jednostek) – co jednak skutkowałoby kilkukrotnym obniżeniem wysokości nowych grantów, czyniąc je nieatrakcyjnymi i nieefektywnymi przy podobnym koszcie obsługi nowego grantu,*
- *ograniczony do określonej liczby wniosków z zasadą "kto pierwszy, ten lepszy", co jednak nie byłoby optymalnym rozwiązaniem. Taka formuła mogłaby dyskryminować mniejsze JST, które często nie są w stanie szybko przygotować i złożyć wniosków. Stałoby to w sprzeczności z celem projektu zakładającym dotarcie do szerokiego spektrum jednostek, w tym tych mniejszych. Z naszej kilkuletniej współpracy z samorządami także w innych projektach (Zdalna Szkoła, Zdalna Szkoła Plus, Cyfrowa Gmina) wiemy, że niestety nie wszystkie JST dysponują odpowiednim potencjałem kadrowym, oraz zasobami niezbędnymi do szybkiej realizacji dodatkowych zadań projektowych.*

Wobec powyższej analizy stwierdziliśmy, że dodatkowy nabór mógłby prowadzić do niskiej efektywności i ryzyka niewykorzystania środków, lub nieosiągnięcia

zakładanych celów. Organizacja dodatkowych naborów w ramach tego Projektu, mogłaby także nie spełniać kryteriów celowości, efektywności i gospodarności wydatkowania środków publicznych. Priorytetem pozostaje skuteczna realizacja Projektu, przy zachowaniu jakości i adekwatności wsparcia.

(akta kontroli str. 22 – 36, 85 – 111, 112 – 119, CD pliki 002, 003, 005, 039)

Do 31 sierpnia 2025 r. prośbę o wydłużenie okresu kwalifikowalności wydatków/realizacji Projektu zgłosiło trzech Grantobiorców:

- Województwo Podlaskie – w związku z wydłużeniem terminu zawarcia umowy z CPPC i tym samym skróceniem okresu, w jakim Grantobiorca przewidywał realizację projektu grantowego;
- Gmina Cieszanów – w związku z równoległą realizacją przez Gminę innego projektu pn. "Przyjazny e-urząd w Cieszanowie" dofinansowanego w ramach priorytetu FEPK.01 „Konkurencyjna i Cyfrowa Gospodarka", działanie FEPK.01.02 „Cyfryzacja programu regionalnego Fundusze Europejskie dla Podkarpacia na lata 2021-2027";
- Starostwo Powiatowe w Mrągowie – w związku z koniecznością ponownej analizy wniosku o dofinansowanie grantu przez nowo wybrany Zarząd Powiatu i zmiany omyłkowo opisanego wskaźnika w zakresie liczby jednostek organizacyjnych Powiatu i liczby usług wsparcia realizowanych przez ekspertów z zakresu cyberbezpieczeństwa.

W I półroczu 2025 r. CPPC otrzymało pięć zgłoszeń od sygnalisty[12] w sprawie potencjalnych nieprawidłowości dotyczących kwalifikowalności wydatków w Projekcie dokonywanych przez Grantobiorców na zakup serwerów, przeznaczonych na zapewnienie cyberbezpieczeństwa, ale jednocześnie wykorzystywanych do obsługi aplikacji dziedzinowych, co było według sygnalisty niezgodne z założeniami Projektu. Sygnalista poinformował o dokonaniu takich zakupów przez JST po analizie kilkudziesięciu upublicznionych postępowań ogłoszonych w ramach Projektu.

CPPC działając jako IP otrzymało również pięć zgłoszeń za pośrednictwem Prezesa Urzędu Zamówień Publicznych (dalej: UZP) w sprawie nieprawidłowości w realizacji przez pięciu Grantobiorców zamówień publicznych (Gmina Węgliniec, Gmina Bierawa, Powiat Strzeliński, Gmina Siechnice oraz Gmina Czastary: znaki spraw: CPPC-D03B00-W04.72.1.6.2.2025/MJ, CPPC-D03B00-W04.72.1.2.3.2025/MJ, CPPC-D03B00-W04.72.2.6.2.2024/MJ[13]. CPPC w odpowiedzi do Prezesa UZP poinformowało, że NASK, zgodnie z procedurą monitorowania i kontroli, na etapie rozliczania Projektu przeprowadzi weryfikację wydatków Grantobiorców. Dodatkowo CPPC poinformowało, że Partner (NASK) przeprowadzi u trzech Grantobiorców (Powiat Strzeliński, Gmina Siechnice oraz Gmina Czastary) w 2025 r. kontrolę doraźną w celu weryfikacji

[12] Sygnalista to osoba, która zgłasza nieprawidłowości, naruszenia prawa lub nadużycia w miejscu pracy, instytucji publicznej lub organizacji.

[13] Zarzuty dotyczyły: niezgodnego z ustawą z dnia 11 września 2019 r. Prawo zamówień publicznych zaniechania podziału zamówień na części, nieprawidłowego opisu przedmiotu zamówienia wskazującego na konkretny produkt i jednego wykonawcę, opisania warunków udziału w postępowaniu w sposób nieproporcjonalny, jak również niecelowego i nierzetelnego wydatkowania środków Unii Europejskiej, zaniechania odrzucenia oferty, która nie spełnia wymagań specyfikacji warunków zamówienia.

zgłoszonych nieprawidłowości. Odnośnie do Gmin Bierawa i Węgliniec poinformowano, że CPPC wspólnie z Partnerem ustali zakres i terminy kontroli, którą Partner będzie prowadził u Grantobiorców.

CPPC działając jako Beneficjent otrzymało jedno zgłoszenie złożone przez przedsiębiorcę dotyczące podejrzenia nieprawidłowości w procedurze wyboru wykonawcy w przetargu organizowanym przez Gminę Miasto Sochaczew. CPPC na dzień zakończenia kontroli było na etapie analizowania sprawy.

Ponadto, CPPC działając jako Beneficjent otrzymało zgłoszenie złożone za pośrednictwem Ministerstwa Funduszy i Polityki Regionalnej przez organizacje pozarządowe dotyczące podejrzenia nieprawidłowości przy przyznaniu dofinansowania beneficjentowi (Gmina Odrzywół) w ramach FERC. Na dzień zakończenia kontroli sprawa była rozpatrywana przez CPPC.

(akta kontroli str. 85 – 111, CD plik 002, 98 - 107)

3. W opracowanym przez CPPC WoD, w pkt H2 „Analiza ryzyka w projekcie", zidentyfikowano łącznie 11 ryzyk dotyczących Projektu, oszacowano prawdopodobieństwo ich wystąpienia, zdefiniowano skutek oraz wskazano mechanizmy zapobiegania. Zidentyfikowane ryzyka dotyczyły braku możliwości wniesienia wkładu własnego przez JST, niedoszacowania lub przeszacowania budżetu Projektu, niewystarczającego poziomu zainteresowania konkursem grantowym, niepoprawnie działającej aplikacji naboru wniosków grantowych, braku odpowiedniej infrastruktury w JST do modernizacji w ramach projektu, niestabilnej sytuacji w obszarze cen towarów, usług oraz kursów walut, problemów z płynnością dostaw rozwiązań IT, braku chęci do użytkowania zakupionych i zmodernizowanych rozwiązań i usług przez JST, problemów z pozyskaniem wykwalifikowanej kadry przez JST do obsługi wdrożonych rozwiązań, opóźnień w realizacji projektu, niepodpisania oraz rozwiązania części umów grantowych. Zidentyfikowane ryzyka w ramach Projektu do dnia zakończenia kontroli nie były aktualizowane.

W „Instrukcji użytkownika Aplikacji WOD2021. Wnioski o dofinansowanie. Wnioskodawca" (stan na dzień 17 marca 2023 r., wersja 1.8) w pkt. 1.2.8. dotyczącym sekcji H „Analiza ryzyka" zawarto tabelę z instrukcją jej wypełnienia umieszczoną w sekcji H2 WoD. W tabeli tej, w opisie dotyczącym rubryki „Mechanizmy zapobiegania" (str. 49), zawarto wymaganie, aby opisać krótko mechanizmy kontrolne, które Beneficjent zamierza zastosować, aby obniżyć opisywane ryzyko. CPPC wskazało we WoD ryzyka, przy czym dla żadnego z nich nie wskazano konkretnych mechanizmów kontrolnych, tj. instrukcji, procedur i narzędzi monitorowania (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

Dla dwóch ryzyk skutkujących opóźnieniem realizacji Projektu Beneficjent wskazał mechanizmy zapobiegania ich wystąpieniu z pominięciem elementów kontroli, które we WoD opisano następująco:

- dla ryzyka dotyczącego problemów z płynnością dostaw rozwiązań IT związanych np. z ograniczeniami gospodarczymi wynikającymi ze zbrojnej agresji Rosji w Ukrainie i obostrzeniami epidemiologicznymi, o dużej sile oddziaływania ryzyka i średnim prawdopodobieństwie wystąpienia - sposób zarządzania ryzykiem poprzez zmiany w harmonogramie Projektu

i dostosowanie go do sytuacji. Łagodzeniem ryzyka będzie poszukiwanie rozwiązań alternatywnych, które mogą zastąpić niedostępne rozwiązania;
- dla ryzyka dotyczącego opóźnienia realizacji Projektu, o dużej sile oddziaływania ryzyka i średnim prawdopodobieństwie wystąpienia - Wnioskodawca planując etapy Projektu założył ramy czasowe obejmujące dodatkowy bufor, uwzględniający nagłe zdarzenia wpływające na czas realizacji zadania. Ponadto Wnioskodawca w przypadku wystąpienia tego ryzyka dokona powtórnej analizy procesu realizacji Projektu, m.in. pod kątem możliwości zaangażowania zespołu projektowego do realizacji wymaganych w tym czasie zadań.

Dyrektor CPPC poinformował, że *dotychczas nie wystąpiło żadne z ryzyk wskazanych we WoD, a Beneficjent na bieżąco kontroluje sytuację i jest przygotowany do podjęcia odpowiednich działań, jeśli pojawi się taka potrzeba*.

(akta kontroli str. 5 – 8, 22 – 47, 52 – 60, 85 – 111, CD pliki 002, 003, 005, 008)

Z ustaleń kontroli wynika, że CPPC posiadało Informacje o problemach, jakie występują w trakcie realizacji Projektu. Beneficjent brał udział w regularnych spotkaniach z Partnerem Projektu, które były organizowane raz w tygodniu. Na spotkaniach omawiane były bieżące tematy związane z realizacją Projektu, postępy prac, trudności i ryzyka, jakie dostrzegają partnerzy wraz z propozycją rozwiązania problemu. Na spotkaniach wspólnie planowano działania na najbliższe tygodnie.

W sporządzonych przez Partnera Projektu notatkach[14], w których zawarto ustalenia z cotygodniowych spotkań z CPPC wskazano problemy związane z realizacją Projektu dotyczące m.in.:

- wydłużenia okresu realizacji Projektu, gdyż coraz więcej JST zgłaszało prośby o wydłużenie okresu kwalifikowalności wydatków/realizacji Projektu. Podjęto decyzję, że zostaną skierowane pisma do JST z informacją o konieczności zakończenia Projektu w założonym terminie;
- kwestii nieprawidłowości zgłaszanych przez sygnalistów na etapie prowadzenia postępowań przetargowych w JST. Postanowiono, że należy uzgodnić z NASK proces kontroli na obsługę tego typ zdarzeń;
- procedury rozliczania wniosków o płatność przez CPPC oraz NASK i ustalenia jak będzie przebiegał ten proces oraz czy będzie on polegał na weryfikacji dokumentów przez dwóch pracowników. Przyjęto, że wskazane jest, aby wnioski były weryfikowane przez dwie osoby.

(akta kontroli str 85 – 111, CD pliki 002, 095, 096)

4. Harmonogram prac nad Projektem określono we WoD. W ramach zmiany WoD wprowadzonej aneksem nr FERC.02.02-IP.01—0001/23-02 wcześniej rozpoczęto realizację zadania nr 4 *Monitorowanie naboru i realizacji projektów grantowych, kontrola projektów grantowych*, lecz pozostało to bez wpływu na termin jego zakończenia. Jednocześnie w toku czynności kontrolnych stwierdzono, że w ramach zadania nr 5 *Ewaluacja, rozliczenie projektu*, którego

[14] Notatki ze spotkań statutowych z Partnerem Projektu (NASK – PIB), na których Partner zgłaszał problemy i sygnalizował ryzyka związane z projektem „Cyberbezpieczny samorząd" – z 12 marca 2025 r., 26 marca 2025 r.

realizację zaplanowano na okres od 1 listopada 2025 r. do 31 grudnia 2027 r., poniesiono wydatki niezgodnie z WoD, tj. przed terminem rozpoczęcia zadania. Na dzień 31 maja 2025 r. wydatki w tym zadaniu (w pozycji 5.2 *Personel projektu – Wynagrodzenia pracowników*) wyniosły 828,3 tys. zł i stanowiło 50% alokacji dla tego zadania (dalszy opis w sekcji *Stwierdzone nieprawidłowości*). Poza ww. zmianami prace były realizowane zgodnie z harmonogramem.

(akta kontroli str. 85 – 111, CD pliki 002, 003, 039)

5. Dokumentacja konkursu grantowego nie przewidywała oceny poziomu cyberbezpieczeństwa w JST na etapie składania wniosków o dofinansowanie grantu. W Regulaminie konkursu grantowego „Cyberbezpieczny samorząd" oraz w załączniku nr 4 do Regulaminu, tj. we wzorze umowy o powierzeniu grantu, nałożono natomiast na Grantobiorców obowiązek przekazywania Partnerowi (NASK) Ankiet Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu Terytorialnego po zawarciu Umowy o powierzenie grantu oraz przy składaniu wniosku rozliczającego Projekt.

Zgodnie § 3 ust. 3 Regulaminu konkursu Grantobiorcy na etapie rozliczenia grantu mieli obowiązek *przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia KRI*[15] oraz zgodnie z określonymi w Regulaminie konkursu warunkami[16], a także dostarczyć raport z tego audytu do NASK wraz z wnioskiem rozliczającym Projekt[17]. W dokumentacji konkursowej, za której przygotowanie odpowiadało CPPC[18], audyty nie zostały w żaden inny sposób ustandaryzowane, co uniemożliwia porównywanie ich ze sobą (np. w skali kraju). W szczególności nie sformułowano obowiązku zamieszczenia w raportach z tych audytów oceny podniesienia poziomu odporności JST na cyberzagrożenia w związku z realizacją Projektu. Ustalenia dokonane w ramach tych audytów nie zostały powiązane z kwalifikowalnością wydatków (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

Ponadto ustalono, że w regulaminie konkursu grantowego oraz na stronach internetowych Projektu w sekcji „Pytania i odpowiedzi" przeznaczonej dla Grantobiorców, brak było jednoznacznego stanowiska CPPC w zakresie jednoczesnego funkcjonowania systemów bezpieczeństwa z systemami dziedzinowymi[19] Grantobiorcy (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 76 – 84, CD pliki 003, 036)

---

[15] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. W sprawie krajowych ram interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, ze zm.), dalej: rozporządzenie KRI z 2012 r.

[16] M.in. zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST miał obejmować zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI z 2012 r. lub zgodność z wymaganiami normy PN-ISO/IEC 27001 (§ 3 ust. 3 pkt 1 Regulaminu konkursu).

[17] Zgodnie z § 4 ust. 10 Regulaminu konkursu.

[18] § 4 ust. 4 pkt 9 umowy o partnerstwie.

[19] Rozumianymi jako niezależne, wyspecjalizowane system informatyczny przeznaczone do obsługi wąskiego i ściśle określonego obszaru funkcjonowania organizacji.

6. W wyniku badania 30 umów zawartych przez CPPC z Grantobiorcami ustalono, że okres liczony od dnia zakończenia oceny WoD do dnia podpisania umowy wynosił od 3 do 8 miesięcy, czyli średnio około pół roku, przy czym okres zawierania tych umów (liczony od dnia otrzymania od Grantobiorców kompletnych i poprawnych dokumentów niezbędnych do podpisania umowy, o których mowa w § 6 ust. 4 Regulaminu konkursu grantowego „Cyberbezpieczny samorząd" do dnia podpisania umowy przez CPPC) wynosił od 14 do 182 dni, czyli średnio około 3 miesięcy. Spowodowało to skrócenie okresu na realizację umów przez Grantobiorców, gdyż zakończenie realizacji umów musi nastąpić do 30 czerwca 2026 r. Najdłuższy okres zawierania umowy miał miejsce w przypadku następujących Grantobiorców: Miasto i Gmina Bochnia - 182 dni, Urząd Marszałkowski Województwa Lubelskiego w Lublinie - 166 dni, Gmina Baranów - 154 dni, Urząd Marszałkowski Województwa Pomorskiego w Gdańsku - 143 dni, Miasto Stołeczne Warszawa - 140 dni.

Dyrektor CPPC podał m.in., że kluczowym powodem takiego stanu rzeczy był wydłużający się proces oceny formalnej i merytorycznej oraz etap przygotowania poprawnej dokumentacji przez JST. Ponadto Dyrektor CPPC podkreślił znaczenie skali całego przedsięwzięcia i liczby pracowników zajmujących się obsługą wniosków i podpisywaniem umów (ok. 23 osób w CPPC i NASK). Dyrektor wskazał też, że długi czas trwania procedury zawarcia umowy nie był efektem bezczynności po stronie Beneficjenta, ale złożonego i rozciągniętego w czasie procesu po stronie Grantobiorcy i Partnera.

(akta kontroli str. 22 – 47, 76-111, 61- 66, CD pliki 002, 003, 036, 038, 111, 112)

7. W ramach nadzoru nad realizacją przez Partnera (NASK) zadań określonych w UoP, CPPC podejmowało działania polegające m.in. na:

- udziale w cotygodniowych spotkaniach statusowych z Partnerem, na których omawiane były bieżące tematy związane z realizacją Projektu, postęp prac, występujące trudności i możliwe ryzyka. W trakcie spotkań planowane były działania na kolejne tygodnie;
- analizie cotygodniowych raportów z realizacji prac, przesyłanych przez Partnera, zawierających m.in. dane z obsługi helpdesk, statystyki z liczby podpisanych umów, zleconych i wypłaconych przelewów, złożonych wniosków o kolejne transze, wniosków końcowych, sprawozdań;
- weryfikacji przekazywanych przez Partnera dokumentów niezbędnych do podpisania umów o powierzenie grantu;
- weryfikacji wniosków o płatność składanych przez Partnera;
- prowadzeniu zestawienia wydatków i środków rozliczonych w Projekcie w celu weryfikacji zaawansowania finansowego Projektu;
- przygotowywaniu we współpracy z Partnerem informacji i instrukcji publikowanych na stronie internetowej Projektu w sekcji „Pytania i Odpowiedzi".

CPPC do dnia zakończenia kontroli, tj. do 5 września 2025 r., nie prowadziło kontroli realizacji Projektu w NASK.

W latach 2023 – 2025 (do 5 września 2025 r.) CPPC działając jako IP przeprowadziło kontrolę CPPC jako Beneficjenta w zakresie działań podejmowanych w Projekcie i faktycznego postępu rzeczowego prac. Zalecenia

pokontrolne zawarte w Informacji Pokontrolnej z 14 marca 2025 r. (FERC.02.02-IP.01-0001/23-003-INF) wskazywały na potrzebę:

- większej staranności przy wypełnianiu wniosku o płatność w zakresie spójności danych. CPPC jako Beneficjent poinformowało, że zwróciło się do Partnera o większą staranność przy składaniu wniosków o płatność i dokładniejsze weryfikowanie przekazywanej dokumentacji;
- powołania Zespołu projektowego, zgodnie z UoP. CPPC jako Beneficjent poinformowało, że powołało zespoły projektowe zgodnie z opisem Beneficjenta i Partnera wskazanymi we WoD, który stanowi załącznik do DoD. W ramach zaleceń pokontrolnych CPPC zobowiązało się opracować zmianę do UoP, które uwzględnią powołanie dwóch odrębnych zespołów projektowych i dołożyć wszelkich starań, aby planowany do podpisania aneks do UoP odzwierciedlał założenia z WoD;
- uzupełniania w kolejnych wnioskach o płatność informacji o nazwę Grantobiorcy i numer umowy o powierzenie grantu, aby zapewnić spójność danych i ścieżkę audytu. CPPC jako Beneficjent poinformowało, że jest na etapie konsultacji z administratorem systemu Teta oraz z dostawcą systemu i w sytuacji, gdy taka zmiana będzie możliwa do wprowadzenia wypełni zalecenie pokontrolne lub znajdzie inne rozwiązanie;
- całościowej weryfikacji i aktualizacji listy rankingowej Grantobiorców oraz ustalenia przez CPPC sposobu rozliczenia aktualnej wysokości przyznanego grantu w przypadku zmian kwot dofinansowania na liście rankingowej dla wszystkich Grantobiorców. CPPC jako Beneficjent poinformowało, że jest na końcowym etapie weryfikacji listy rankingowej i że zamieści poprawną listę rankingową na stronie internetowej. Ponadto, do każdego wniosku o płatność dołączy odrębne zestawienie wypłaconych grantów z podziałem na środki UE i BP oraz z informacją o numerze transzy, co umożliwi IP dokładną weryfikację wypłat;
- wprowadzenia i stosowania przez Partnera miesięcznych kart czasu pracy dla personelu zaangażowanego w realizację Projektu, które potwierdzą faktyczne zaangażowanie w Projekt w danym miesiącu i będą stanowiły podstawę do wyliczenia kwalifikowanej części wynagrodzenia i jego rozliczania w Projekcie. CPPC jako Beneficjent poinformowało Partnera o konieczności stosowania miesięcznych kart czasu pracy i konsultowało z Partnerem i IP formę prowadzenia ewidencji przez Partnera.

W ramach konkursu grantowego „Cyberbezpieczny Samorząd" został przewidziany do realizacji i przeprowadzony jeden nabór wniosków. Beneficjent zrealizował zadania w zakresie przygotowania konkursu grantowego i naboru do Projektu zgodnie z harmonogramem określonym we WoD. We wniosku tym wskazano, że rozpoczęcie realizacji Projektu nastąpiło 1 lipca 2023 r., przygotowanie konkursu grantowego trwało od 1 do 19 lipca 2023 r., a uruchomienie naboru rozpoczęto 19 lipca 2023 r. Według wyjaśnień Dyrektora CPPC, *datę rozpoczęcia realizacji Projektu, czyli 1 lipca 2023 r., Beneficjent wyznaczył wcześniej niż datę uruchomienia naboru, ponieważ w tym czasie prowadził prace przygotowawcze. Obejmowały one m.in. przygotowanie dokumentacji naborowej dla Grantobiorców oraz inne działania niezbędne do sprawnego uruchomienia konkursu. Następnie 19 lipca 2023 r. Beneficjent uruchomił konkurs grantowy*.

(akta kontroli str. 27 – 36, CD pliki 003, 005)

8. Beneficjent we WoD przewidział 11 wskaźników produktu[20] i cztery wskaźniki rezultatu[21]. Do dnia zakończenia czynności kontrolnych CPPC działając jako Beneficjent nie zgłosiło CPPC działającemu jako Instytucja Pośrednicząca faktu nieosiągnięcia jednego wskaźnika produktu - *Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji* i jednego wskaźnika rezultatu - *Liczba JST wspartych w zakresie cyberbezpieczeństwa* spośród wskaźników określonych we WoD. Zważywszy na to, że nabór wniosków grantowych zakończył się 14 grudnia 2023 r., mając na względzie postanowienia § 22 ust. 2 pkt 2 DoD, w myśl których IP może uchylić decyzję o dofinansowaniu w przypadku, gdy Beneficjent nie zrealizował wskaźników produktu i rezultatu określonych we wniosku o dofinansowanie, niezgłoszenie do dnia zakończenia czynności kontrolnych faktu nieosiągnięcia ww. wskaźników należy uznać za nierzetelne. Jest to o tyle istotne, że z postanowień § 19 ust. 4 DoD wynika, iż zmiany w obrębie wskaźników zdefiniowanych we WoD wymagają akceptacji Instytucji Pośredniczącej i są wprowadzane aneksem do decyzji (dalszy opis w sekcji *Stwierdzone nieprawidłowości*).

Postanowienia § 4 ust. 4 pkt 11 UoP nakładają na partnera wiodącego – CPPC – obowiązek monitorowania wskaźników zadeklarowanych we wniosku o dofinansowanie. Z pkt 7 i 8 sekcji 2.1.3 „Wytycznych dotyczących monitorowania postępu rzeczowego realizacji programów na lata 2021 – 2027" Ministra Funduszy i Polityki Regionalnej[22] (dalej: Wytyczne dot. monitorowania) wynika, że informacje o poziomie osiąganych wskaźników powinny być składane przez Beneficjenta do IP wraz z wnioskami o płatność. Jednak do 1 lipca 2025 r. nie dopełniono tego obowiązku (dalszy opis w sekcji *Stwierdzone nieprawidłowości*). Do tego dnia składano jedynie informację o wskaźniku rezultatu „Liczba JST wspartych w zakresie cyberbezpieczeństwa".

(akta kontroli str. 37 - 43, 61 – 66, 67 – 75, CD pliki 001, 003, 004, 006, 111)

9. Do 31 sierpnia 2025 r. nie wystąpiły opóźnienia w realizacji Projektu. Według wyjaśnień Dyrektora CPPC, dotychczas nie wystąpiły problemy w realizacji

---

[20] Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych – 0, Liczba podmiotów wspartych w zakresie cyberbezpieczeństwa - 2, liczba podmiotów wspartych w zakresie rozwoju usług, produktów i procesów cyfrowych - 2, liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym (łącznie) – 2807, liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym – kobiety: 421, liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym – mężczyźni: 2386, liczba pracowników IT podmiotów wykonujących zadania publiczne niebędących pracownikami IT objętych wsparciem szkoleniowym (łącznie) – 2807, liczba pracowników IT podmiotów wykonujących zadania publiczne niebędących pracownikami IT objętych wsparciem szkoleniowym – kobiety: 2230, liczba pracowników IT podmiotów wykonujących zadania publiczne niebędących pracownikami IT objętych wsparciem szkoleniowym – mężczyźni: 577, liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji – 2807, Wartość usług, produktów i procesów cyfrowych opracowanych dla przedsiębiorstw - 0.

[21] Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych - 5614, liczba JST wspartych w zakresie cyberbezpieczeństwa - 2807, liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST – 140, Użytkownicy nowych i zmodernizowanych usług, produktów i procesów cyfrowych opracowanych przez przedsiębiorstwa - 0.

[22] https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/prawo-i-dokumenty/wytyczne/wytyczne-dotyczace-monitorowania-postepu-rzeczowego-realizacji-programow-na-lata-2021-2027/

Projektu, skutkujące zagrożeniem jego pełnej realizacji. Postępy prac, występujące trudności i ewentualne problemy związane z realizacją Projektu były omawiane na bieżąco w trakcie organizowanych co tydzień spotkań CPPC i NASK.

(akta kontroli str. 85 - 111, CD plik 002)

10. Do dnia zakończenia kontroli w CPPC działającym jako Beneficjent, CPPC działające jako IP przeprowadziło kontrolę dotyczącą realizacji działań w ramach Projektu (zalecenia IP omówiono w pkt 7 niniejszego wystąpienia pokontrolnego). Ponadto, kontrolę w tym zakresie przeprowadziła także Izba Administracji Skarbowej w Warszawie[23] (dalej: IAS). W trakcie audytu projektu FERC.02.02-IP.01-0001/23 „Cyberbezpieczny Samorząd" IAS ustaliła, że CPPC jako Beneficjent wykazało we wnioskach o płatność nr FERC.02.02-IP.01-0001/23-002 i nr FERC.02.02-IP.01-0001/23-003 zawyżone o 18 360,81 zł koszty pośrednie. Zgodnie z DoD, Beneficjent mógł rozliczyć koszty pośrednie według stawki ryczałtowej w wysokości 15% kwalifikowanych bezpośrednich kosztów personelu[24]. W odpowiedzi na wyniki audytu, CPPC zgłosiło zastrzeżenia dotyczące sposobu rozliczania kosztów pośrednich. W odpowiedzi na zastrzeżenia, IAS podtrzymała pierwotne ustalenie. Beneficjent dokonał po tym korekty kosztów pośrednich pomniejszających te koszty o kwotę 18 360,81 zł.

(akta kontroli str. 27 – 36, CD plik 003, 005)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Wskazane w analizie ryzyka mechanizmy zapobiegania dla 11 zidentyfikowanych ryzyk nie zostały opisane w sposób gwarantujący bezzwłoczne podjęcie działań zaradczych, co było działaniem nierzetelnym.

Zamiast wskazania mechanizmów kontrolnych, które pozwoliłyby na pozyskiwanie wiedzy na temat zagrożeń w obrębach poszczególnych ryzyk, CPPC zawarło w analizie ryzyka ogólne stwierdzenia, niewskazujące konkretnych działań, procedur, osób odpowiedzialnych ani narzędzi monitorowania. CPPC na etapie realizacji Projektu, w trakcie kontroli NIK, podjęło próbę wypracowania mechanizmów kontrolnych i procedur reagowania.

Dyrektor CPPC wyjaśnił m.in., że od momentu uruchomienia naboru CPPC wdraża konkretne działania ograniczające ryzyko opóźnień w realizacji Projektu, polegające m.in. na wdrożeniu infolinii projektowej i adresu e-mail, strony internetowej Projektu, czy też organizacji webinarów dla Grantobiorców.

Zdaniem NIK, opisane w analizie ryzyka mechanizmy zapobiegania nie identyfikują faktycznego zagrożenia, a przeciwdziałają skutkom zaistnienia ryzyka opóźnienia w realizacji Projektu dopiero w reakcji na zgłoszenie z zewnątrz. Świadczy o tym fakt, że do dnia 31 sierpnia 2025 r. odnotowano

---

[23] Audyt operacji nr FERC.02.02-IP.01-0001/23-004.

[24] Zgodnie z Wytycznymi dotyczącymi kwalifikowalności wydatków na lata 2021-2027. Jednocześnie zapisy podrozdziału 3.10. pkt 9 lit c) ww. wytycznych wskazują, że rozliczenie następuje według określonej stawki ryczałtowej odnoszonej do kwalifikowalnych kosztów będących podstawą rozliczenia.

szereg sygnałów mogących świadczyć o występowaniu istotnych zagrożeń dla terminowej realizacji Projektu, w tym: trzy jednostki samorządu terytorialnego wystąpiły z wnioskami o przedłużenie okresu kwalifikowalności wydatków lub realizacji Projektu, zarejestrowano pięć zgłoszeń sygnalisty dotyczących wątpliwości w zakresie kwalifikowalności wydatków, pięć zgłoszeń wpłynęło za pośrednictwem Prezesa UZP i dotyczyło możliwych nieprawidłowości w zakresie zamówień publicznych realizowanych przez pięć różnych JST, dodatkowo jedno zgłoszenie zostało przekazane bezpośrednio do CPPC jako Beneficjenta. W reakcji na te zagrożenia CPPC przesłało rekomendacje do JST o konieczności zakończenia Projektu zgodnie z dotychczasowymi założeniami i uruchomiło proces opracowywania procedury kontroli zasygnalizowanych nieprawidłowości w zakresie zamówień publicznych. Należy zauważyć, że zgłaszane problemy w obszarze realizacji zamówień publicznych dotyczą jednego z kluczowych ryzyk wpływających na ewentualne opóźnienia w realizacji Projektu, a działania CPPC polegające na uzgadnianiu procesu kontrolnego podejmowane są dopiero po zaistnieniu zdarzeń mogących mieć wpływ na terminową realizację Projektu.

(akta kontroli str. 5 – 8, 22 – 47, 52 – 60, 85 – 111, CD pliki 002, 003, 005, 008)

2. Wydatki w wysokości 828,3 tys. zł w ramach zadania nr 5 *Ewaluacja, rozliczenie projektu* poniesiono niezgodnie z WoD, tj. przed planowanym terminem jego rozpoczęcia. Realizację ww. zadania zaplanowano na okres od 1 listopada 2025 r. do 31 grudnia 2027 r., a wydatki zaczęto ponosić już w I kwartale 2025 r.

Dyrektor CPPC potwierdził*, że zadanie nr. 5 zgodnie z aktualną wersją Wniosku o dofinansowanie powinno rozpocząć się 1.11.2025 r. Jednakże już w styczniu 2025 r. do Partnera Projektu wpłynęły pierwsze wnioski rozliczające grant, co wymusiło wcześniejsze rozpoczęcie czynności w tym zakresie (...) Beneficjent przekaże do Instytucji Pośredniczącej wniosek o zgodę na wprowadzenie zmiany terminu rozpoczęcia zadania nr 5 przy planowanym aneksie do Decyzji o dofinansowaniu. W odniesieniu do danych zawartych we wniosku o płatność nr 10 – Partner błędnie przypisał wszystkie koszty osobowe z 2025 r. do zadania nr 5, podczas gdy część z tych wynagrodzeń dotyczy faktycznie zadań realizowanych w ramach zadania nr 3. Błąd ten został zidentyfikowany i Beneficjent przygotuje wyjaśnienia do Instytucji Pośredniczącej, wraz z prośbą o możliwość korekty wniosku nr 10 i odpowiednie przypisanie kosztów do zadań nr 3 i 5.*

(akta kontroli pliki str. 85 – 111, CD 002, 003, 039)

3. W dokumentacji konkursu grantowego nie przewidziano oceny poziomu cyberbezpieczeństwa u Grantobiorców na etapie składania przez nich wniosków o grant oraz nie przyjęto zasady, aby powiązać osiągnięty poziom cyberbezpieczeństwa po zakończeniu prac w ramach grantu z kwalifikowalnością wydatków, co było nierzetelne. Należy podkreślić, że celem Projektu grantowego jest wsparcie JST w zakresie realizacji usług publicznych na drodze teleinformatycznej, poprzez zwiększenie cyfryzacji jednostek samorządu terytorialnego wraz z jednostkami podległymi w kontekście zwiększenia poziomu cyberbezpieczeństwa.

Dyrektor CPPC wyjaśnił, że *na etapie składania wniosków przewidziano ocenę poziomu cyberbezpieczeństwa na podstawie kryteriów nr 6 i 8. Kolejnym etapem oceny jest dwukrotne dostarczenie ankiety dojrzałości cyberbezpieczeństwa -*

zarówno po podpisaniu umowy, jak i na etapie rozliczenia grantu. (…) Do udziału w naborze były uprawnione wszystkie jednostki samorządu terytorialnego (dalej JST). Dla każdej JST określono maksymalną kwotę grantu o jaką mogły się ubiegać. Tym sposobem JST nie konkurowały ze sobą np. wysokością zadeklarowanego poziomu cyberbezpieczeństwa (…) Bezpośrednie powiązanie wyników oceny ankiety dojrzałości z kwalifikowalnością wydatków zdaniem Beneficjenta jest nieuzasadnione. W ramach Projektu przyjmuje się, że poziom bezpieczeństwa jednostki podniesie się względem stanu, gdyby Projekt nie został w niej wdrożony. Często wdrożenie nowych rozwiązań może skutkować utrzymaniem poziomu bezpieczeństwa lub dostosowaniem do zmieniających się regulacji (w tym nadchodzącej implementacji dyrektywy NIS2) obowiązujących Jednostki Samorządu Terytorialnego w jednostce.

W opinii NIK, brak oceny poziomu cyberbezpieczeństwa na etapie składania wniosków przez JST o przyznanie grantu może przyczynić się do niezbyt efektywnego wykorzystywania środków w Projekcie, ponieważ CPPC jako Beneficjent nie może ocenić tego w jakim stopniu przyznany grant podniósł poziom bezpieczeństwa JST. W ramach kryterium 6. *Zasadność kosztów w Projekcie* „weryfikacji podlega czy Wnioskodawca grantowy wystarczająco uzasadnił potrzebę wskazanych wydatków oraz ich racjonalność w kontekście celu projektu oraz potrzeb Wnioskodawcy", zaś w ramach kryterium 8. *Opis koncepcji projektu* „weryfikacji podlega, czy Wnioskodawca grantowy przedstawił opis koncepcji Projektu zawierający informacje: o potrzebach Wnioskodawcy grantowego w zakresie cyfryzacji urzędu w tym zwiększenia poziomu bezpieczeństwa informacji urzędu (…), celach i efektach Projektu, w tym w odniesieniu do celów FERC". W żadnym z ww. kryteriów nie jest zatem oceniany wzrost poziomu cyberbezpieczeństwa, który będzie skutkiem realizacji Projektu grantowego. W § 3 ust. 3 Regulaminu konkursu grantowego przewidziano konieczność przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji i przekazanie raportu z tego audytu wraz z wnioskiem rozliczającym projekt, lecz nie połączono jego wyników z oceną wzrostu poziomu cyberbezpieczeństwa osiągniętym w wyniku realizacji Projektu grantowego i kwalifikowalnością wydatków w tym zakresie.

(akta kontroli str. 76 – 84, CD pliki 003, 036)

4. W Projekcie, w ramach projektów grantowych, dopuszczono możliwość jednoczesnego funkcjonowania na serwerach zarówno systemów dziedzinowych jak i systemów bezpieczeństwa, co należy uznać za niezgodne z § 15 pkt 1 rozporządzenia KRI stanowiącym, że systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk. Współistnienie tych systemów zwiększa ryzyko eskalacji (podniesienia) uprawnień, ponieważ aplikacja dziedzinowa – nawet jeśli nie jest dostępna z Internetu – może stanowić wektor ataku w sieci wewnętrznej. Dodatkowo prowadzi to do potencjalnego konfliktu o zasoby serwera, co obniża stabilność i niezawodność systemów bezpieczeństwa.

NIK zauważa, że celem grantu jest zwiększenie poziomu bezpieczeństwa, a zatem serwer powinien być wykorzystywany do uruchamiania systemów bezpieczeństwa wdrożonych w ramach projektu grantowego, a wszelkie dodatkowe aplikacje powinny działać na odrębnej infrastrukturze.

Dyrektor CPPC wyjaśnił, że *Beneficjent dopuścił taką możliwość, ponieważ kategoryczne wyłączenie takiej możliwości, a przez to potencjalny brak kwalifikowalności wydatku, byłoby niewskazane w wypadku stanu wyższej konieczności, w którym każda decyzja pozwalająca na przywrócenie możliwości świadczenia usług warta jest rozważenia. (...) Utrzymanie ciągłości pracy systemów jest ważnym celem mieszącym się w obszarze odporności na zagrożenia. Dopuszcza się, że w ramach serwera fizycznego zainstalowany jest system wirtualizacyjny. (...) Analogicznie mogą funkcjonować również systemy dziedzinowe, które zostaną zainstalowane na oddzielnych innych maszynach wirtualnych w ramach tego samego serwera fizycznego (w tym w klastrach wysokiej dostępności). (...) Należy jednak zauważyć, że o ile zakup serwerów i oprogramowanie zapewniające bezpieczeństwo są ujęte w katalogu kosztów kwalifikowalnych, to już użytkowanie oraz obsługa wszelkich aplikacji dziedzinowych, ich komponentów oraz serwerów bazodanowych na zakupionym sprzęcie będą uznawane za koszty niekwalifikowalne w ramach projektu.*

Mając na względzie ogólne cele programu FERC, jak wsparcie transformacji cyfrowej kraju przez realizację przedsięwzięć, które zapewnią m.in. skuteczne działanie krajowego systemu cyberbezpieczeństwa, jak i cel szczegółowy interwencji określony dla działania 2.2, tj. inwestycje zwiększające poziom bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych, nie sposób zgodzić się z podejściem zaprezentowanym przez CPPC. Separacja systemów dziedzinowych i bezpieczeństwa pozwala ograniczyć zakres ataków i zmniejszyć skalę ewentualnych strat, ułatwia zarządzanie całą infrastrukturą i nie wpływa negatywnie na jej wydajność[25]. Kluczowe jest bowiem faktyczne i możliwe najwyższe zwiększenie poziomu cyberbezpieczeństwa. Zdaniem NIK, przyjęte w konkursie grantowym rozwiązanie narusza zasadę separacji funkcji, zgodnie z którą systemy bezpieczeństwa i aplikacje użytkowe nie powinny współdzielić zasobów tego samego serwera.

(akta kontroli str. 76 – 84, CD pliki 003, 036)

5. Do dnia zakończenia czynności kontrolnych CPPC działając jako Beneficjent nie zgłosiło CPPC działającemu jako Instytucja Pośrednicząca faktu braku możliwości osiągnięcia jednego wskaźnika produktu - *Liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji* i jednego wskaźnika rezultatu - *Liczba JST wspartych w zakresie cyberbezpieczeństwa* spośród określonych we WoD. Zważywszy na to, że nabór wniosków grantowych zakończył się 14 grudnia

[25] Wynika to z zasad zarządzania IT i jest zgodne normami i dobrymi praktykami, np. ISO 27001 i NIST SP 800-53 rev.5. W tej ostatniej normie zawarto następujące reguły kontrolne: SC-2 – Separation of System and User Functionality - Mechanizmy bezpieczeństwa (security functions) powinny być realizowane oddzielnie od funkcjonalności użytkowej systemu; SC-3 – Security Function Isolation Funkcje bezpieczeństwa muszą być izolowane od innych funkcji w systemie informatycznym; SA-14 – Criticality Analysis (uzupełniająca) – Podkreśla konieczność identyfikacji i odseparowania elementów krytycznych (np. usług bezpieczeństwa) od reszty systemu.

2023 r., mając na względzie postanowienia § 22 ust. 2 pkt 2 DoD, w myśl których IP może uchylić decyzję o dofinansowaniu w przypadku, gdy Beneficjent nie zrealizował wskaźników produktu i rezultatu określonych we wniosku o dofinansowanie, niezgłoszenie do dnia zakończenia czynności kontrolnych faktu nieosiągnięcia ww. wskaźników należy uznać za nierzetelne. Jest to o tyle istotne, że z postanowień § 19 ust. 4 DoD wynika, iż zmiany w obrębie wskaźników zdefiniowanych we WoD wymagają akceptacji Instytucji Pośredniczącej i są wprowadzane aneksem do decyzji.

W toku kontroli ustalono, że dwa ww. wskaźniki, których wartość ustalono na poziomie 2807, na pewno nie zostaną osiągnięte, gdyż w ramach jedynego naboru grantowego w ramach Projektu złożono 2614 wniosków, a obecnie realizowanych jest 2490 umów o powierzeniu grantu, z czego wynika, że możliwe jest osiągnięcie 88,7% zakładanego poziomu wskaźników.

Dyrektor CPPC wyjaśnił, że *wskaźnik odnoszący się do liczby Grantobiorców (2807) nie zostanie osiągnięty. Różnica ta jest trwała i nieodwracalna, ponieważ nabór nie będzie powtórzony (...) Beneficjent podjął działania mające na celu dostosowanie wskaźników projektu do faktycznego poziomu jego realizacji. Trwają robocze rozmowy z Instytucją Pośredniczącą, Instytucją Zarządzającą oraz Ministerstwem Cyfryzacji w zakresie planowanej aktualizacji Decyzji o dofinansowanie, w tym Wniosku o dofinansowanie. Planowana zmiana obejmuje zarówno korektę wskaźnika liczby Grantobiorców, jak i proporcjonalne zmniejszenie pozostałych wskaźników bezpośrednio powiązanych z liczbą JST*. (...) *Obecnie Beneficjent na nowo szacuje wartości wskaźników i aktualizuje treść wniosku o dofinansowanie*.

(akta kontroli str. 37 - 43, 61 – 66, 67 – 75, CD pliki 001, 003, 004, 006, 111)

6. CPPC działające jako Beneficjent do 1 lipca 2025 r. nie sprawozdawało na bieżąco we wnioskach o płatność wartości wskaźników, co naruszało postanowienia § 4 ust. 4 pkt 11 UoP oraz pkt 7 i 8 sekcji 2.1.3 „Wytycznych dot. monitorowania. Powyższe postanowienia nakładają na Beneficjentów obowiązek bieżącego monitorowania postępu rzeczowego, czemu służą m.in. wartości wskaźników sprawozdawane we wnioskach o płatność.

Dyrektor CPPC poinformował, że: *Beneficjent od początku realizacji projektu raportuje postępy zgodnie z wymaganiami wynikającymi z Decyzji o dofinansowanie oraz zapisów Wniosku o dofinansowanie. Do tej pory raportował do Instytucji Pośredniczącej jedynie wskaźnik „Liczba JST wspartych w zakresie cyberbezpieczeństwa", ponieważ był on bezpośrednio powiązany z wypłatami grantów. Pozostałe wskaźniki Beneficjent będzie mógł raportować na bieżąco po zatwierdzeniu przez Partnera wniosków o rozliczenie grantu złożonych przez JST. Obecnie Partner zatwierdził 15 wniosków rozliczających grant (dane na dzień 18.07.2025 r.), na podstawie których Beneficjent wskaże wartości osiągniętych wskaźników we wniosku o płatność nr 11. Beneficjent zaktualizuje ten wniosek i uzupełni dane wskaźnikowe.*

Należy zauważyć, że dopiero w dwunastym Wniosku o płatność (za okres od 1 do 30 lipca 2025 r.), składanym w trakcie kontroli NIK, Beneficjent uzupełnił dane w zakresie wartości osiągniętych wskaźników, pomimo że przed wskazanym okresem zatwierdził już pierwsze wnioski JST o rozliczenie grantu.

(akta kontroli str. 37 - 43, 61 – 66, 67 – 75, CD pliki 001, 003, 004, 006, 111)

IV. Wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące wnioski:

Wnioski

1. Dokonanie aktualizacji analizy ryzyka w Projekcie w zakresie mechanizmów kontrolnych.
2. Ponoszenie wydatków na zadania zaplanowane w Projekcie zgodnie z harmonogramem.
3. W przypadku prowadzenia kolejnych projektów dotyczących cyberbezpieczeństwa, uwzględnienie oceny poziomu cyberbezpieczeństwa na etapie składania wniosków o przyznanie grantu, a także po zakończeniu jego realizacji w powiązaniu z kwalifikowalnością wydatków.
4. Zapewnienie w przypadku realizacji kolejnych projektów w zakresie wdrażania rozwiązań informatycznych wymogu separacji systemów dziedzinowych i bezpieczeństwa.
5. Bieżące informowanie IP o potrzebie niezbędnych zmian w obrębie wskaźników produktu i rezultatu Projektu oraz wystąpienie do IP o zmiany Decyzji o dofinansowanie i Wniosku o dofinansowanie w tym zakresie.
6. Bieżące sprawozdawanie we wnioskach o płatność wartości wskaźników.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne sporządzono w postaci elektronicznej z użyciem kwalifikowanych podpisów elektronicznych.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Departamentu Administracji Publicznej. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, września 2025 r.

Kontrolerzy

Tomasz Kwitowski

Doradca techniczny

podpis/podpisano elektronicznie

Ewa Bimkiewicz

Specjalista kontroli państwowej

podpis/podpisano elektronicznie

Najwyższa Izba Kontroli

Departament Administracji Publicznej

Dyrektor

Bogdan Skwarka

podpis/podpisano elektronicznie