Minister
Cyfryzacji

BBKN.WBK.0811.8.2025
Warszawa, 28 stycznia 2026 r.

Pan
Radosław Nielek
Dyrektor
Naukowa i Akademicka Sieć Komputerowa-
Państwowy Instytut Badawczy

WYSTĄPIENIE POKONTROLNE

Na podstawie art. 6 ust. 3 pkt 1 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[1] (dalej: *ustawa o kontroli*) w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym (dalej: NASK-*PIB* lub *Instytut*, j*ednostka*), z siedzibą przy ul. Kolskiej 12, 01-045 Warszawa została przeprowadzona kontrola w zakresie realizacji zadań obronnych, ze szczególnym uwzględnieniem obowiązków administracji publicznej w zakresie pozamilitarnego wsparcia systemu bezpieczeństwa narodowego w latach 2024-2025.

Czynności kontrolne prowadzone były w dniach od 10 października do 31 grudnia 2025 r. przez zespół kontrolny w składzie:

- Sylwia Półtorak – Główny specjalista w Wydziale Bezpieczeństwa i Kontroli Biura Bezpieczeństwa, Kontroli i Nadzoru,
- Agnieszka Popłonkowska – Główny specjalista w Wydziale Bezpieczeństwa i Kontroli Biura Bezpieczeństwa, Kontroli i Nadzoru.

NASK-PIB jest instytutem badawczym realizującym zadania z zakresu tworzenia i rozwoju nowoczesnej cyberprzestrzeni w Rzeczypospolitej Polskiej. Instytut prowadzi działalność naukowo-badawczą w obszarach cyberbezpieczeństwa, sztucznej inteligencji oraz technologii przetwarzania danych w chmurze.

Instytut wspiera podmioty gospodarcze w zakresie ochrony przed zagrożeniami cybernetycznymi poprzez opracowywanie i wdrażanie rozwiązań bezpieczeństwa, realizację audytów bezpieczeństwa teleinformatycznego oraz doradztwo w procesach transformacji cyfrowej. Jednocześnie realizuje zadania na rzecz administracji publicznej, w tym w szczególności zapewnia dostęp do internetu dla placówek oświatowych, tworzy i rozwija systemy zarządzania dokumentacją w administracji państwowej oraz prowadzi szkolenia z zakresu cyberbezpieczeństwa.

Ponadto NASK-PIB podejmuje działania na rzecz ochrony obywateli, w szczególności poprzez przeciwdziałanie oszustwom internetowym, identyfikację i usuwanie stron internetowych zawierających treści niezgodne z obowiązującymi przepisami prawa oraz

[1] Dz. U. z 2020 r. poz. 224

telefon: +48 22 245 54 45
adres email: sekretariat.BBKN@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

realizację działań edukacyjnych zwiększających świadomość zagrożeń w środowisku cyfrowym..

NASK-PIB jest instytucją naukowo-badawczą oraz operatorem sieci i usług teleinformatycznych, pełniącą kluczową rolę w zapewnieniu bezpieczeństwa cyberprzestrzeni w Polsce. Działalność NASK-PIB obejmuje rozwój technologii informatycznych, monitorowanie zagrożeń cybernetycznych, zarządzanie strategicznymi zasobami internetowymi oraz prowadzenie działań prewencyjnych i interwencyjnych w zakresie ochrony infrastruktury krytycznej.

Instytut zapewnia wsparcie administracji publicznej, przedsiębiorstwom oraz użytkownikom indywidualnym, dostarczając narzędzia i wiedzę niezbędną do skutecznego przeciwdziałania cyberzagrożeniom. Dzięki połączeniu funkcji badawczo-rozwojowych z działalnością operacyjną, NASK-PIB przyczynia się do wzmocnienia obronności kraju w cyberprzestrzeni.

Instytut działa na podstawie:

- Ustawy o instytutach badawczych[2],
- Zarządzenia nr 5/93 Przewodniczącego Komitetu Badań Naukowych z dnia 14 grudnia 1993 r. w sprawie utworzenia Naukowej i Akademickiej Sieci Komputerowej [3],
- Rozporządzenia Rady Ministrów z dnia 7 czerwca 2017 r. w sprawie nadania NASK statusu państwowego instytutu badawczego[4],
- Statutu NASK-PIB[5],
- Ustawy o krajowym systemie cyberbezpieczeństwa[6]: NASK-PIB pełni obowiązki jednego z Zespołów Reagowania na Incydenty Komputerowe (CSIRT), co wynika z przepisów tej ustawy, nadającej mu konkretne zadania w zakresie cyberbezpieczeństwa państwa.

Do zadań Instytutu należy w szczególności:[7] prowadzenie badań naukowych i prac rozwojowych; przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki, wdrażanie wyników badań naukowych i prac rozwojowych w usługach świadczonych między innymi na potrzeby organów bezpieczeństwa i porządku publicznego; bezpieczeństwa państwa oraz bezpieczeństwa jednostek infrastruktury krytycznej; dokonywanie oceny zgodności, prowadzenie procesów certyfikacji oraz działalności normalizacyjnej; prowadzenia działań w cyberprzestrzeni, w tym testów bezpieczeństwa.

Ponadto Instytut może prowadzić inną działalność w zakresie dopuszczonym w *Statucie*[8].

---

[2] Dz.U. z 2024 r. poz. 534.
[3] Dziennik Urzędowy KBN nr 7, poz. 33.
[4] Dz.U. 2017 poz. 1193.
[5] Decyzja Nr 1 Ministra Cyfryzacji z dnia 21 stycznia 2025 r. w sprawie zatwierdzenia zmian w statucie Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (
[6] Dz.U. 2018 poz. 1560.
[7] § 6 Statutu NASK-PIB.
[8] § 7 Statutu NASK-PIB.

Kierownictwo jednostki kontrolowanej:

Organami NASK-PIB są:

- Dyrektor,
- Rada Naukowa.

Dyrektorem Instytutu jest dr inż. Radosław Nielek.
Funkcje zastępców Dyrektora pełnią:

- Mariusz Madejczyk (Dyrektor ds. Nowych Technologii dla Polityk Publicznych),
- Magdalena Tarczewska-Szymańska (Dyrektor ds. Procesów Administracyjnych),
- Adam Marczyński (Dyrektor ds. Cyberbezpieczeństwa i Innowacji),
- dr Małgorzata Olszewska (Dyrektor ds. Projektów Infrastrukturalnych i Edukacyjnych).

Kontrola została przeprowadzona w trybie zwykłym, zgodnie z ustawą o kontroli w administracji rządowej. Kontrola została ujęta w Planie kontroli do realizacji przez Biuro Bezpieczeństwa, Kontroli i Nadzoru w Ministerstwie Cyfryzacji w 2025 r.

Weryfikacją zostały objęte następujące zagadnienia:

1. **Organizacja, zarządzanie i nadzór nad zadaniami obronnymi:**
    1.1. Tworzenie warunków organizacyjnych i technicznych do planowania i wykonywania zadań obronnych.
    1.2. Realizacja planowania operacyjnego i programowania obronnego.
2. **Realizacja zadań obronnych w jednostce kontrolowanej:**
    2.1. Przygotowanie do realizacji zadań wynikających ze stanów gotowości obronnej państwa.
    2.2. Realizacja wyłączenia pracowników z obowiązku pełnienia służby wojskowej w razie ogłoszenia mobilizacji i w czasie wojny na potrzeby organów administracji publicznej i innych jednostek organizacyjnych.

I. OCENA OGÓLNA KONTROLOWANEGO OBSZARU

Przygotowanie jednostki do realizacji zadań obronnych, w szczególności w zakresie organizacji, zarządzania i nadzoru nad zadaniami obronnymi, a także przygotowania jednostki kontrolowanej do wykonywania tych zadań w czasie zagrożenia bezpieczeństwa państwa lub wojny oceniono pozytywnie.

Instytut realizował zadania obronne w sposób celowy (w tym zgodny z ich założeniami, odpowiedni i skuteczny), legalny (w tym zgodnie z obowiązującymi wymogami) oraz rzetelny (w tym z zachowaniem należytej staranności).

II. OCENY I USTALENIA SZCZEGÓŁOWE

1. Organizacja, zarządzanie i nadzór nad zadaniami obronnymi.

1.1. Tworzenie warunków organizacyjnych i technicznych do planowania i wykonywania zadań obronnych.

W ramach kontroli niniejszego zagadnienia zweryfikowano w jaki sposób zapewniono właściwą organizację oraz skuteczne planowanie, zarządzanie oraz nadzór nad realizacją zadań obronnych.

W trakcie czynności kontrolnych stwierdzono, że jednostka zapewniła odpowiednie warunki organizacyjne i techniczne do planowania i wykonywania zadań obronnych.
Przygotowanie struktur organizacyjnych do realizacji zadań obronnych zapewniono:

- Zarządzeniem nr 391 Dyrektora NASK-PIB z dnia 1 lipca 2019 r. w sprawie Regulaminu organizacyjnego NASK-PIB. W Regulaminie określono m.in. nową strukturę oraz zadania komórek organizacyjnych. Począwszy od wejścia w życie ww. zarządzenia, prowadzenie spraw związanych z realizacją zadań obronnych przez NASK przypisano do Centrum Zarządzania i Polityki Informacyjnej (dalej: CZiPI)[9];
- Zarządzeniem nr 392 Dyrektora NASK-PIB z dnia 1 lipca 2019 r . w sprawie schematu organizacyjnego NASK-PIB. W załączniku nr 2 do Zarządzenia ustalono i wprowadzono szczegółowy opis zadań komórek organizacyjnych, zgodnie z którym na poziomie działów, za prowadzenie spraw obronnych NASK odpowiedzialny był Zespół Ochrony Fizycznej i Infrastruktury, wchodzący w skład Działu Ochrony Informacji Niejawnych (dalej: DOIN)[10].

Od lipca 2019 r. regulamin organizacyjny oraz schemat organizacyjny NASK-PIB zmieniany był kilkukrotnie, przy czym realizacja zadań obronnych pozostała każdorazowo w kompetencji CZiPI - DOIN, włącznie do obecnie obowiązującego Zarządzenia nr 719 Dyrektora NASK-PIB z dnia 30 września 2025 r. w sprawie wprowadzenia zmian w Regulaminie organizacyjnym[11].
Zgodnie z zapisami Zarządzenia nr 720 Dyrektora NASK-PIB z dnia 30 września 2025 r. w sprawie zmiany schematu organizacyjnego od dnia 1 października 2025 r. za prowadzenie spraw obronnych NASK odpowiedzialni są Administratorzy BSP i Inspektorzy w DOIN[12].
Potwierdzono, że osoby odpowiedzialne za te zadania posiadają kwalifikacje do wykonywania ww. obowiązków[13].

W ramach oceny infrastruktury technicznej do wykonywania dokumentów niejawnych stwierdzono, że NASK-PIB posiada Kancelarię Tajną oraz infrastrukturę techniczną umożliwiającą przetwarzanie informacji do klauzuli ŚCIŚLE TAJNE włącznie.

Jednostka posiada:

---

[9] Punkt V § 19 Regulaminu, który stanowi, że „Centrum Zarzadzania i Polityki Informacyjnej odpowiada w szczególności za prowadzenie spraw związanych z realizacja zadań obronnych przez NASK (...)".
[10] Punkt I 4) c) Opisu Zadań Komórek Organizacyjnych NASK-PIB zgodnie ze schematem organizacyjnym, stanowiącym załącznik nr 2 do Zarządzenia nr 392.
[11] Rozdział VI § 33 pkt 4) Regulaminu Organizacyjnego, stanowiącego załącznik do Zarządzenia Dyrektora NASK-PIB nr 719 z dnia 30 września 2025 r.
[12] Rozdział I, pkt. 3, lit. b) załącznika nr 2 do Zarządzenia Dyrektora NASK-PIB nr 720 z dnia 30 września 2025 r.
[13] Wyjaśnienia Dyrektora NASK-PIB z dnia 21 października 2025 r., znak DAW.091.9.2025.

- Plan Organizacji Kancelarii Tajnej Międzynarodowej w NASK-PIB obsługującej informacje niejawne EU i NATO oznaczone klauzulami Secret UE/EU Secret, Confidentiel UE/EU Confidential, Restreint UE/EU Restricted, NATO Secret, NATO Confidential, NATO Restricted. Plan został zatwierdzony przez krajową władzę bezpieczeństwa[14]. Kancelaria tajna międzynarodowa w NASK-PIB zostanie wpisana do ewidencji kancelarii tajnych międzynarodowych prowadzonej w Departamencie Ochrony Informacji Niejawnych ABW po uzyskaniu przez Instytut świadectw bezpieczeństwa przemysłowego.
- Świadectwo Akredytacji Bezpieczeństwa Systemu Teleinformatycznego do przetwarzania informacji niejawnych do klauzuli: ściśle tajne, NATO Secret, Secret UE/EU Secret ważne do 3 grudnia 2027 r.[15]
- Świadectwo Akredytacji Bezpieczeństwa Systemy Teleinformatycznego do przetwarzania informacji niejawnych do klauzuli poufne ważne do 27 października 2029 r.[16]

Stwierdzone nieprawidłowości.

W kontrolowanym obszarze nie stwierdzono nieprawidłowości.

Ocena kontrolowanego obszaru.

Ocena cząstkowa obszaru jest pozytywna.

1.2. Realizacja planowania operacyjnego i programowania obronnego.

NASK-PIB uczestniczył w obowiązku planowania operacyjnego i programowania obronnego, w wyniku którego sporządzono:

- Plan operacyjny funkcjonowania Naukowej i Akademickiej Sieci Komputerowej- Państwowego Instytutu Badawczego w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny (POF). Plan został opatrzony klauzulą POUFNE. POF został zatwierdzony przez Ministra Cyfryzacji[17];
- Wypis z aneksu aktualizacyjnego POF DAR-I, opatrzony klauzulą ZASTRZEŻONE;
- Tabelę realizacji zadań operacyjnych, opatrzoną klauzulą ZASTRZEŻONE;
- Karty realizacji zadań operacyjnych, opatrzone klauzulą ZASTRZEŻONE.

Dokumentacja niejawna o klauzuli ZASTRZEŻONE została udostępniona kontrolerom MC do wglądu w Kancelarii Tajnej NASK-PIB.

Z uwagi na brak stosownych upoważnień po stronie zespołu kontrolującego do dostępu do dokumentów oznaczonych klauzulą POUFNE, Plan operacyjny

[14] Pismo Agencji Bezpieczeństwa Wewnętrznego Departament Ochrony Informacji Niejawnych znak: D-1507/2025 z 8 stycznia 2025r.
[15] Świadectwo nr 190/2025 z dnia 27 maja 2025 r. wydane przez Agencję Bezpieczeństwa Wewnętrznego dla systemu NASK-ST1.
[16] Świadectwo nr 156/2024 z dnia 29 października 2024 r. wydane przez Agencję Bezpieczeństwa Wewnętrznego dla systemu NASK-ST-2.
[17] Pismo Kancelarii Prezesa Rady Ministrów znak BOIN-Pf-623/2022 z 10 marca 2022 r.

funkcjonowania został wyłącznie okazany, bez zapewnienia możliwości zapoznania się z jego treścią.

W trakcie czynności kontrolnych zweryfikowano karty realizacji zadań operacyjnych i stwierdzono, że karty sporządzono do wszystkich zadań operacyjnych ujętych w *Tabeli realizacji zadań operacyjnych*.

Ponadto stwierdzono, że jednostka realizowała szkolenia obronne, w tym ćwiczenia dla pracowników. Szkolenia obronne dla pracowników organizowane były na podstawie zatwierdzonych przez Dyrektora NASK-PIB „Planów Szkolenia Obronnego na dany rok". Okazano Plan Szkolenia Obronnego na 2024 i 2025 r.

Instytut wypełniał także Narodowy Kwestionariusz Pozamilitarnych Przygotowań Obronnych Działu Administracji Rządowej Cyfryzacja dla części dotyczącej NASK-PIB, jako wkład do Kwestionariusza sporządzanego przez Ministra Cyfryzacji[18].

Stwierdzone nieprawidłowości.

W kontrolowanym obszarze nie stwierdzono nieprawidłowości.

Ocena kontrolowanego obszaru.

Ocena cząstkowa obszaru jest pozytywna.

2. Realizacja zadań obronnych w jednostce kontrolowanej

2.1 Przygotowanie do realizacji zadań wynikających ze stanów gotowości obronnej państwa - ocena procedur uruchamiania stałego dyżuru i organizacji jego funkcjonowania.

Funkcjonowanie stałego dyżuru w NASK-PIB jest uregulowane Instrukcją stałego dyżuru, która określa:

1. Zakres zadań dyżuru, obejmujący m.in. komunikację decyzji uprawnionych organów oraz prowadzenie ewidencji działań.
2. Sposób uruchamiania i odwoływania dyżuru – decyzję podejmuje Dyrektor NASK-PIB lub osoba przez niego upoważniona.
3. Skład osobowy dyżuru, obejmujący kierownika dyżuru, dyżurnych oraz pomocników dyżurnego.
4. Tryb pracy dyżuru – całodobowo na dwie zmiany po uruchomieniu.

W toku czynności kontrolnych ustalono, że Instrukcja stałego dyżuru obowiązująca w NASK-PIB zawiera postanowienie umożliwiające aktualizację treści załączników w przypadku zmian organizacyjnych lub kadrowych, bez konieczności ponownego wydawania dokumentu. Z informacji przekazanych przez kontrolowaną jednostkę wynika, że dane organizacyjne oraz personalne ujęte w Instrukcji stałego dyżuru są aktualne.

Jednocześnie stwierdzono, że Instrukcja stałego dyżuru została opracowana w oparciu o podstawę prawną, która na dzień prowadzenia czynności kontrolnych nie była już obowiązująca. Instrukcja odwołuje się do rozporządzenia Rady Ministrów z dnia 21 września 2004 r. w sprawie gotowości obronnej państwa

[18] Kwestionariusz podpisany przez Dyrektora NASK-PIB 6 lutego 2025 r.

(Dz.U. 2004 nr 219 poz. 2218), uchylonego z dniem 29 marca 2025 r. rozporządzeniem Rady Ministrów z dnia 18 marca 2025 r. w sprawie gotowości obronnej państwa (Dz.U. 2025 poz. 355), oraz do zarządzenia nr 20 Ministra Cyfryzacji z dnia 15 czerwca 2016 r. w sprawie systemu stałego dyżuru, które utraciło moc obowiązującą.

Prowadzenie próbnych uruchomień i wdrożenie Stałego Dyżuru.

Na podstawie analizy przedłożonej dokumentacji oraz informacji uzyskanych od kontrolowanej jednostki, ustalono, że próbne uruchomienia Stałego Dyżuru w NASK-PIB są realizowane zgodnie z obowiązującymi planami szkoleń obronnych. W ramach Planu Szkolenia Obronnego na 2024 r. przeprowadzono wewnętrzny trening Stałego Dyżuru w dniu 15 lipca 2024 r. Natomiast zgodnie z Planem Szkolenia Obronnego na 2025 r. zrealizowano wewnętrzny trening Stałego Dyżuru w IV kwartale 2025 r.

Realizacja ćwiczeń Stałego Dyżuru ma charakter systematyczny i służy bieżącej weryfikacji obowiązujących procedur oraz przygotowaniu personelu do wykonywania zadań w warunkach podwyższonej gotowości obronnej państwa.

Wyposażenie pomieszczenia Stałego Dyżuru w sprzęt łączności.

Na podstawie informacji uzyskanych od NASK-PIB oraz ustaleń dokonanych na miejscu stwierdzono, że pomieszczenie Stałego Dyżuru jest wyposażone w wymagane rozporządzeniem[19] środki i systemy łączności.

Ustalono, że urządzenia i systemy łączności są utrzymywane w stanie sprawnym i wykorzystywane w bieżącej działalności Instytutu. Materiały eksploatacyjne zapewnia Pion Informatyki i Telekomunikacji. Wyposażenie pomieszczenia Stałego Dyżuru w sprzęt łączności umożliwia realizację zadań dyżurnych oraz wspiera zachowanie ciągłości ich wykonywania.

Awaryjne źródło zasilania pomieszczenia Stałego Dyżuru.

Ustalono, że NASK-PIB posiada zasilanie sieciowe z dwóch niezależnych kierunków oraz zintegrowany system zasilania gwarantowanego, obejmujący system UPS oraz agregat prądotwórczy wyposażony w funkcję automatycznego uruchamiania. Do systemu zasilania gwarantowanego podłączona jest infrastruktura wykorzystywana w pomieszczeniu Stałego Dyżuru.

Agregat prądotwórczy poddawany jest regularnym testom – raz w miesiącu na sztucznym obciążeniu oraz raz w roku w rzeczywistym układzie zasilania. Stosowane rozwiązania zapewniają gotowość Stałego Dyżuru do nieprzerwanej pracy w sytuacjach awaryjnych.

Dostęp do wykazów telefonów alarmowych i kontaktów.

Dostęp do wykazów telefonów alarmowych oraz kontaktów do służb, instytucji i osób funkcyjnych zapewniają pracownicy Działu Ochrony Informacji Niejawnych

[19]Rozporządzenie Rady Ministrów z dnia 18 marca 2025 r. w sprawie gotowości obronnej państwa (Dz.U. 2025 poz. 355).

NASK-PIB. Aktualizacja danych dokonywana jest po otrzymaniu informacji o zmianach, co – według wyjaśnień jednostki – pozwala na utrzymanie wykazów w stanie odpowiadającym przekazywanym informacjom.

Rejestrowanie meldunków i zdarzeń oraz bezpieczeństwo dokumentacji.

Meldunki i zdarzenia rejestrowane są w Dzienniku Dyżurów oraz w Dzienniku ewidencji przyjmowanych i przekazywanych zadań operacyjnych, przedsięwzięć systemu zarządzania kryzysowego, decyzji, meldunków i raportów. Ciągłość i prawidłowość prowadzenia dokumentacji nadzorowana jest przez Kierownika Zespołu oraz pracowników Działu Ochrony Informacji Niejawnych NASK-PIB.

Dokumentacja przetwarzana jest w Strefie Ochronnej III, umożliwiającej przetwarzanie informacji niejawnych do klauzuli „Zastrzeżone" włącznie. Pomieszczenie Stałego Dyżuru zabezpieczone jest systemem sygnalizacji włamania i napadu, systemem kontroli dostępu, systemem przeciwpożarowym oraz systemem dozoru wizyjnego. Zastosowane środki techniczne i organizacyjne w istotnym stopniu ograniczają ryzyko naruszenia bezpieczeństwa informacji oraz nieuprawnionego dostępu do pomieszczenia dyżurnego.

Środki ochrony indywidualnej.

NASK-PIB nie zidentyfikował szczególnych zagrożeń w pomieszczeniu Stałego Dyżuru, które wymagałyby stosowania środków ochrony indywidualnej. Pomieszczenie wyposażone jest w gaśnice, których stan techniczny i gotowość do użycia podlegają okresowej kontroli, realizowanej zgodnie z harmonogramem nadzorowanym przez Dział Administracji NASK-PIB.

Warunki pracy całodobowej w pomieszczeniu Stałego Dyżuru.

Pomieszczenie Stałego Dyżuru posiada oświetlenie naturalne i sztuczne, w tym oświetlenie awaryjne, klimatyzację z funkcjami chłodzenia, ogrzewania, osuszania i wentylacji, a także centralne ogrzewanie. Zapewniono dostęp do zaplecza socjalnego z wodą oraz urządzeniami kuchennymi, a także do zaplecza sanitarnego, zlokalizowanego w bezpośrednim sąsiedztwie pomieszczenia Stałego Dyżuru. Zastosowane rozwiązania umożliwiają pracę personelu dyżurnego w trybie całodobowym.

Stwierdzone nieprawidłowości.

W kontrolowanym obszarze nie stwierdzono nieprawidłowości.

Ocena kontrolowanego obszaru.

Ocena cząstkowa obszaru jest pozytywna.

2.2 Wyłączenie pracowników z obowiązku pełnienia czynnej służby wojskowej

Ustalono, że NASK-PIB prowadzi działania związane z wyłączeniem swoich pracowników z obowiązku pełnienia czynnej służby wojskowej w razie ogłoszenia mobilizacji lub w czasie wojny. W jednostce określono stanowiska kluczowe dla funkcjonowania NASK-PIB w zakresie realizacji zadań związanych z Infrastrukturą

Krytyczną, w tym m.in.: Dyrektora NASK-PIB, właściwą Dyrekcję, pracowników CERT oraz administratorów systemów teleinformatycznych.

Na dzień przeprowadzania czynności kontrolnych wyreklamowano 61 pracowników NASK-PIB, przy czym liczba ta może ulegać zmianom w zależności od aktualizacji stanowisk kluczowych oraz decyzji organów wojskowych. Dokumentacja dotycząca wniosków o wyłączenie, decyzji organów wojskowych, zarządzeń kierownika jednostki oraz ewidencji osób podlegających wyłączeniu prowadzona jest i zabezpieczona w Kancelarii Tajnej NASK-PIB.

Jednostka realizuje obowiązki związane z wyłączeniem pracowników z czynnej służby wojskowej, co przyczynia się do zachowania ciągłości działania NASK-PIB w sytuacjach kryzysowych.

Stwierdzone nieprawidłowości.

W kontrolowanym obszarze nie stwierdzono nieprawidłowości.

Ocena kontrolowanego obszaru.

Ocena cząstkowa obszaru jest pozytywna.

Biorąc pod uwagę ustalenia i oceny przedstawione w Wystąpieniu, zalecam Panu Dyrektorowi aktualizację Instrukcji stałego dyżuru w zakresie podstawy prawnej jej opracowania.

Proszę Pana Dyrektora o przedstawienie, w terminie 60 dni od daty otrzymania Wystąpienia, informacji o sposobie wykonania zaleceń. Jednocześnie informuję, że od Wystąpienia nie przysługują środki odwoławcze.

Z up. Sebastian Strawa
Dyrektor Biura Bezpieczeństwa, Kontroli i Nadzoru
w Ministerstwie Cyfryzacji
/dokument podpisany elektronicznie/