



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.106.2026
Warszawa, 29 czerwca 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 1 czerwca br. Pośla na Sejm RP Pana Bartosza Józefa Kownackiego w sprawie katastrofalnych luk w procesie koordynacji działań w zakresie cyberbezpieczeństwa najważniejszych osób w państwie, realizowanych w ramach systemu ochrony państwa przez wyspecjalizowane służby, zespoły reagowania oraz instytucje rządowe (interpelacja nr 17433)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

Ad 1) Czy aktualnie faktycznie funkcjonuje system ochrony cybernetycznej dedykowany do osłony najważniejszych osób w państwie?

Ad 2) Który minister w aktualnej Radzie Ministrów odpowiada bezpośrednio za jego funkcjonowanie?

Ad 3) Która z instytucji państwowych (Krajowy System Cyberbezpieczeństwa (KSC) zarządzany przez Ministerstwo Cyfryzacji, CSIRT GOV (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) prowadzony przez Agencję Bezpieczeństwa Wewnętrznego, struktury Służby Ochrony Państwa, czy może policyjne Centralne Biuro Zwalczania Cyberprzestępczości) jest odpowiedzialna za organizację, nadzór i realizację owego systemu?

Ad 4) Czy system ochrony najważniejszych osób w państwie zawiera określone elementy:

- Wydzielone zespół/zespoły osobowe (liczba)?
- Wydzielone systemy IT i łączności zapewniające wymianę danych pomiędzy zespołami /członkami zespołu w trybie całodobowym(jakie i ile)?
- Wypracowane procedury pozyskiwania danych z wszystkich instytucji w trybie online(jakie)?
- Zespół analityków, stosowne zabezpieczenie sprzętowe, programowe itp. umożliwiające analizę danych kluczowych (np. weryfikacja i przypisanie adresów zgłoszeń do ochraniających obiektów) w trybie online (ile i jakie)?
- Możliwości techniczne (np. narzędzia AI) umożliwiające natychmiastową reakcję systemu ochrony (w przypadku prowokacji wobec Prezydenta RP pomiędzy pierwszym wezwaniem „do pożaru”, a drugim wezwaniem „do nieprzytomnej osoby”, minęło 15 minut)?

Odpowiadając na pytania nr 1-4 należy wskazać, że cyberbezpieczeństwo Rzeczypospolitej Polskiej, w tym najważniejszych osób w państwie, jest zapewniane w ramach rozwiązań przewidzianych w ustawie o krajowym systemie

cyberbezpieczeństwa¹ oraz innych aktów prawnych, w tym m.in. ustaw kompetencyjnych poszczególnych służb odpowiedzialnych za bezpieczeństwo państwa. W szczególności należy wskazać na funkcjonowanie trzech zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego, których zakres właściwości jest określony w art. 26 ust. 5–7 UKSC, a ich zadania w art. 26 ust. 3. Zgodnie z tymi przepisami CSIRT-em właściwym dla administracji państwowej jest CSIRT GOV (z wyłączeniem resortu obrony narodowej, dla którego właściwy jest CSIRT MON).

Jednocześnie podmioty publiczne będące podmiotami kluczowymi lub podmiotami ważnymi w rozumieniu UKSC są zobowiązane, na podstawie art. 8 tejże ustawy, do zapewnienia odpowiedniego poziomu cyberbezpieczeństwa, w szczególności poprzez:

- wdrażanie adekwatnych środków technicznych i organizacyjnych służących zarządzaniu ryzykiem w systemach informacyjnych,
- zapewnienie bezpieczeństwa łańcucha dostaw usług i systemów teleinformatycznych,
- stosowanie mechanizmów ochrony poczty elektronicznej, w tym zabezpieczeń przed phishingiem, spoofingiem, złośliwym oprogramowaniem oraz nieuprawnionym dostępem,
- prowadzenie monitorowania systemów teleinformatycznych i wykrywania incydentów,
- zgłaszanie incydentów właściwym zespołom CSIRT oraz podejmowanie działań zapobiegawczych i naprawczych,
- stosowanie polityk bezpieczeństwa, kontroli dostępu oraz szkoleń użytkowników w zakresie bezpiecznego korzystania z poczty elektronicznej i narzędzi komunikacji.

Organy właściwe do spraw cyberbezpieczeństwa dla sektora podmiotów publicznych określone są w art. 41a UKSC, a zadania tych organów w art. 42.

Kwestie cyberbezpieczeństwa, w tym w administracji publicznej i w odniesieniu do najważniejszych osób państwie są przedmiotem działań w ramach Połączonego Centrum Operacyjne Cyberbezpieczeństwa (PCOC), które zapewnia bieżącą koordynację wymiany informacji, monitorowanie sytuacji cyberbezpieczeństwa oraz spójność działań podejmowanych przez podmioty KSC, zgodnie z art. 62a UKSC. Działania o charakterze operacyjnym i wspierania reagowania na incydenty realizowane są przez CSIRT-y poziomu krajowego (CSIRT GOV, CSIRT NASK, CSIRT MON) oraz inne właściwe służby i instytucje, zgodnie z ich ustawowymi kompetencjami, przy zachowaniu mechanizmów współpracy i wymiany informacji w ramach PCOC.

Należy dodać, że w praktyce ochrona najważniejszych osób w państwie w ramach KSC opiera się w głównej mierze na działaniach dwóch wyspecjalizowanych służb. Służba Ochrony Państwa (SOP) odpowiada za bezpośrednią ochronę fizyczną i teleinformatyczną (w tym tzw. urządzeń końcowych) najważniejszych osób w państwie (m.in. Prezydenta, Premiera, Marszałków Sejmu i Senatu) oraz zapobiega atakom, m.in. fizycznym i technicznym, skierowanym przeciwko nim. W kontekście zagadnienia dotyczącego ochrony najważniejszych osób w państwie, warto nadmienić, że zgodnie ustawą o Służbie Ochrony Państwa² Komendant SSOP, w drodze zarządzenia, z zachowaniem przepisów prawa o ochronie informacji niejawnych, określa sposoby, metody i formy podejmowanych czynności i działań przez SOP w zakresie nieobjętym

¹ Ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20 z późn. zm.) dalej jako (UKSC)

² art. 16 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2025 r. poz. 34, z późn. zm.)

innymi regulacjami. Jednocześnie należy zwrócić uwagę, że zgodnie z art. 63 ust. 1 ww. ustawy, informacje o metodach, formach i ewentualnie podejmowanych przez SOP czynnościach podlegają ochronie.

Z kolei ABW odpowiada przede wszystkim za osłonę kontrwywiadowczą tych osób oraz, w ramach zadań CSIRT GOV, monitoruje cyberprzestrzeń pod kątem badania incydentów wymierzonych w administrację publiczną.

Niezależnie od powyższego, Ministerstwo Cyfryzacji we współpracy z NASK realizuje program „SecureV”, obejmujący działania o charakterze prewencyjnym i edukacyjnym w obszarze cyberbezpieczeństwa, skierowane do najważniejszych osób w państwie oraz pracowników administracji publicznej zajmujących kluczowe stanowiska.

Ad 5) Czy w związku z faktem że Prokuratura Okręgowa w Gdańsku prowadząca śledztwo w sprawie fałszywego zgłoszenia o zagrożeniu zdrowia i życia w mieszkaniu w Gdańsku (sprawa dotyczy rodziny prezydenta Karola Nawrockiego) przekazała dochodzenie do Centralnego Biura Zwalczania Cyberprzestępczości (CBZC), to właśnie ta ostatnia instytucja przejęła wiodącą rolę w zakresie cyberbezpieczeństwa Prezydenta RP?

Ad 6) Czy powyższe delegowanie zadań do Policji stanowi o braku zaufania do kompetencji ABW (to ta struktura odpowiada ustawowo za kontrwywiadowczą ochronę najważniejszych osób w państwie, posiada wyodrębniony do tego pion operacyjny, prowadzi CSIRT GOV i odpowiednie uprawnienia śledcze)?

Ad 7) Czy też przekazanie do prowadzenia dochodzenia strukturom Policji spowodowane jest faktem, że nie mamy do czynienia z elementem działań wywiadowczych tylko brutalną prowokacją polityczną wobec Prezydenta RP?

Odpowiadając na pytania nr 5-7 należy zaznaczyć, że Szef Agencji Bezpieczeństwa Wewnętrznego prowadzi Zespół reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, który odpowiada za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze wskazanym w art. 26 ust. 7 ustawy o krajowym systemie cyberbezpieczeństwa. Jednym z jego podstawowych zadań jest monitorowanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa, systemów teleinformatycznych, objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych, właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w ustawie o zarządzaniu kryzysowym³.

Kwestia powierzenia CBZC przez Prokuraturę Okręgową w Gdańsku prowadzenia śledztwa dotyczącego tzw. fałszywych alarmów pozostaje poza gestią wskazanych podmiotów. Wskazana jednostka Prokuratury jest wyłącznym dysponentem informacji w przedmiotowym zakresie. Aktualnie w odniesieniu do fałszywych zgłoszeń, o których mowa w interpelacji, ABW – w ramach współpracy z Policją – podejmuje stosowne czynności weryfikacyjne. Należy również podkreślić, że wyniki prowadzonych przez funkcjonariuszy ABW ustaleń, w trybie art. 18 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, przekazywane są na bieżąco właściwym adresatom.

Niezależnie od powyższego, należy wskazać że śledztwo w sprawie fałszywego zgłoszenia o zagrożeniu życia i zdrowia w mieszkaniu w Gdańsku prowadzi Prokuratura

³ art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. 2026 poz. 574)

Okręgowa Warszawa-Praga w Warszawie. Podmiotem właściwym do udzielenia informacji w przedmiotowej sprawie jest zatem prokurator prowadzący to postępowanie.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych