Ministerstwo
Obrony Narodowej

Sekretarz Stanu
Paweł BEJDA

160. ROCZNICA URODZIN
GEN. BRONI TADEUSZA
JORDAN-ROZWADOWSKIEGO

BMON-WP.053.978.2026/In-449-26/SW
Warszawa, 20.10.2026 r.

Pan Włodzimierz CZARZASTY
Marszałek Sejmu Rzeczypospolitej Polskiej

Do wiadomości: Dyrektor Departamentu Spraw Parlamentarnych w KPRM

ePuap

Dotyczy: interpelacji nr 20134 Pana Posła Michała Jacha wraz z grupą posłów w sprawie naruszenia procedur bezpieczeństwa teleinformatycznego w 16. Dolnośląskiej Brygadzie Obrony Terytorialnej

Szanowny Panie Marszałku,

odpowiadając, z upoważnienia Ministra Obrony Narodowej, na interpelację nr 20134 Pana Posła Michała Jacha wraz z grupą posłów w sprawie naruszenia procedur bezpieczeństwa teleinformatycznego w 16. Dolnośląskiej Brygadzie Obrony Terytorialnej, uprzejmie proszę o przyjęcie poniższych informacji.

Na początku należy sprostować, iż obecnie obowiązującą nazwą systemu, do którego nawiązuje treść interpelacji, jest Usługa Podstawowa ARCUS (UP ARCUS), która nie jest systemem teleinformatycznym w myśl art. 2 pkt 6 ustawy z dnia 10 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r., poz. 1209), lecz funkcjonującą w ramach takiego systemu teleinformatycznego usługą podstawową przeznaczoną do wykorzystania przez wszystkich użytkowników.

System teleinformatyczny, w którym jest uruchomiona UP ARCUS, posiada opracowaną i zatwierdzoną dokumentację bezpieczeństwa teleinformatycznego. Również UP ARCUS ma własną, zatwierdzoną dokumentację bezpieczeństwa usługi. W związku z tym Dowódca 16. Dolnośląskiej Brygady Obrony Terytorialnej (16. DBOT) nie musiał opracowywać odrębnej dokumentacji bezpieczeństwa dla lokalizacji systemu wraz z UP ARCUS.

Dokumentacja systemu zawiera procedury bezpiecznej eksploatacji, w tym zasady korzystania z kont użytkowników w sytuacji, gdy użytkownik z jednostki A pracuje w jednostce B przy stacji roboczej tej drugiej jednostki. Procedury te dopuszczają logowanie się na konto właściwe dla danej jednostki i korzystanie z usług (w tym UP ARCUS) przypisanych do tego konta. Postępowanie zgodne z tymi procedurami nie stanowi naruszenia przepisów o ochronie informacji niejawnych ani procedur bezpieczeństwa. W opisywanym w interpelacji przypadku użytkownik posiadał dwa odrębne konta w systemie — jedno przypisane do jednostki A, drugie do jednostki B — i logował się wyłącznie przy użyciu konta właściwego dla danej jednostki.

W UP ARCUS nie ma pojęcia nieuprawnionej stacji roboczej. Dostęp do baz danych i dokumentów jest realizowany na poziomie grup uprawnień, a pojedynczy użytkownik jest przypisany do określonej grupy. Jeśli użytkownik ma nadane uprawnienia do danej bazy lub dokumentu, jego dostęp jest uprawniony niezależnie od lokalizacji urządzenia, z którego łączy się użytkownik. Mechanizmy bezpieczeństwa zastosowane w UP ARCUS uniemożliwiają nawiązanie połączenia z urządzenia nieautoryzowanego - czynność można wykonać wyłącznie z urządzenia autoryzowanego i uprawnionego.

Ponadto informuję, że systemy eksploatowane w 16. DBOT mają na bieżąco aktualizowaną dokumentację bezpieczeństwa oraz są akredytowane przez organizatora systemu.

Z wyrazami szacunku

Paweł BEJDA

/dokument podpisany kwalifikowanym podpisem elektronicznym/