PART IS

IS.I.OR.100 Zakres stosowania (IS.AR.100))

Urząd Lotnictwa Cywilnego

Rzeszów 2.09.2025

Agenda prezentacji

1. Przykłady zagrożeń
2. Organizacje objęte Part IS - kogo obejmuje
3. Podstawy prawne i dokumenty doradcze - daty wejścia w życie
4. Cele Part IS - wprowadzenie do przepisów
5. ISO 27001
6. Więcej przykładów
7. Podsumowanie

Przykłady zagrożeń bezpieczeństwa informacji w lotnictwie

- Ataki na systemy pokładowe
  - Hakowanie systemów awioniki
- Zagrożenia w łańcuchu dostaw
  - Fałszowanie oprogramowania pokładowego
  - Nieautoryzowana ingerencja w części lotnicze
- Zagrożenia dla infrastruktury lotniskowej
  - Ataki ransomware
  - Ataki DDoS (Distributed Denial of Service)

2017 – testowe włamanie do Boeinga 757 – specjaliści z DHS (Department of Homeland Security) wykazali, że można przejąć kontrolę nad niektórymi funkcjami samolotu zdalnie.

2020 – atak ransomware na Garmin – firma dostarczająca systemy nawigacyjne dla lotnictwa ogólnego została sparaliżowana przez złośliwe oprogramowanie.

"BadUSB" – Gdy Pendrive Staje Się Klawiaturą

Spreparowany Pendrive: Mikrokontroler przeprogramowany – udaje klawiaturę (HID).
Podłączenie: Komputer rozpoznaje go jako nową, zaufaną klawiaturę.
Automatyczne Polecenia: "Wpisuje" złośliwe komendy (np. pobranie malware, kradzież danych, modyfikacja systemu).

Dlaczego Jest Groźny?

- Omija tradycyjne antywirusy (nie jest skanowany jak dysk).
- Wykorzystuje zaufanie systemu do urządzeń HID.
- Szybki, zautomatyzowany, wygląda niewinnie.

Potencjalne Konsekwencje (Lotnictwo):

- Kompromitacja systemów diagnostycznych, dokumentacji (np. fałszywe AMM), kradzież haseł.
- Infekcja komputerów, kradzież danych.
- W skrajnych przypadkach – wpływ na systemy krytyczne.

Jak możemy się chronić?

Jaka jest najlepsza linia obrony, którą TY możesz wdrożyć, aby zapobiec ponad 80% naruszeń danych?

P4s5w0rds!

Bezpieczeństwo Informacji

Co to jest Bezpieczeństwo Informacji?

Ochrona poufności, integralności i dostępności informacji.
Zapewnienie, że informacje są dostępne tylko dla upoważnionych osób (**poufność**).
Gwarancja, że informacje są dokładne i kompletne (**integralność**).
Zapewnienie, że upoważnieni użytkownicy mają dostęp do informacji, kiedy jej potrzebują (**dostępność**).

https://www.nist.gov/image/cia-triad

Organizacje objęte Part IS

Zarządzający lotniskami i płytą postojową

Koncesjonowani przewoźnicy lotniczy (ORO)

Zatwierdzone organizacje szkoleniowe (ATO)

Operatorzy szkolnych urządzeń symulacji lotu (ORA)

Organizacje podlegające załącznikowi III do Rozporządzenia 2017/373 (AMT/ANS)

Instytucje świadczące usługi U-Space

Organizacje obsługi technicznej 145 i zarządzania ciągłą zdatnością do lotu CAMO

Organizacje DOA i POA (projektujące i produkujące)

Bezzałogowe statki powietrzne

Organizacje szkolące i centra medycyny lotniczej kontrolerów ruchu lotniczego

Centra medycyny lotniczej dla załóg lotniczych

Przykłady organizacji nieobjętych Part IS

Zatwierdzone organizacje szkoleniowe (ATO) – tylko szkolenia teoretyczne

Operatorzy UAS (bezzałogowych statków powietrznych) w kategorii „open” i „specific”

Organizacje CAMO, Part 145 zajmujące się tylko statkami poniżej 2000 kg, balony, szybowce.

Organizacje Part 147

Dzięki zasadzie proporcjonalności wymagania można dostosować do skali działalności oraz faktycznego poziomu ryzyka.

https://ulc.gov.pl/aktualnosci/nowe-materialy-doradcze-dotyczace-przepisow-part-is

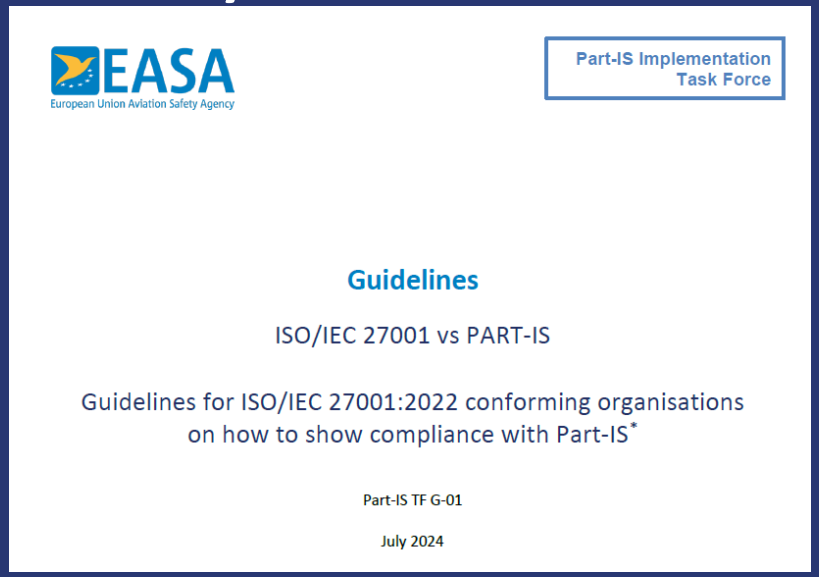
PART IS Information Security

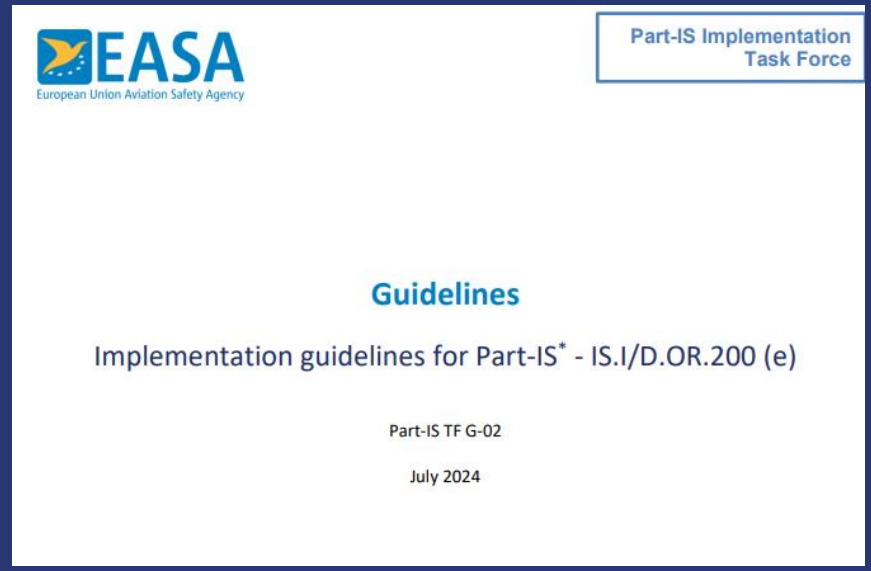
Rozporządzenia Part-IS

- Przepisy europejskie
  - 16.10.2025 → Rozporządzenie **2022/1645** (Part IS dla organizacji POA, DOA dla ELA 2, operatorzy lotnisk i zarządzający płytą)
  - 22.02.2026 → Rozporządzenie **2023/203** (Part IS dla pozostałych organizacji, nadzoru)
- Wytyczne EASA
  - AMC
  - GM

https://www.easa.europa.eu/community/topics/easy-access-rules-part-published - Easy Acces Rules

Materiały doradcze





https://www.easa.europa.eu/community/topics/part-implementation-task-force-deliverables

PART IS - CELE

Part-IS (Information Security) wprowadza wymagania dotyczące zarządzania ryzykiem bezpieczeństwa informacji, które mogą mieć potencjalny wpływ na bezpieczeństwo lotnicze (Aviation Safety).

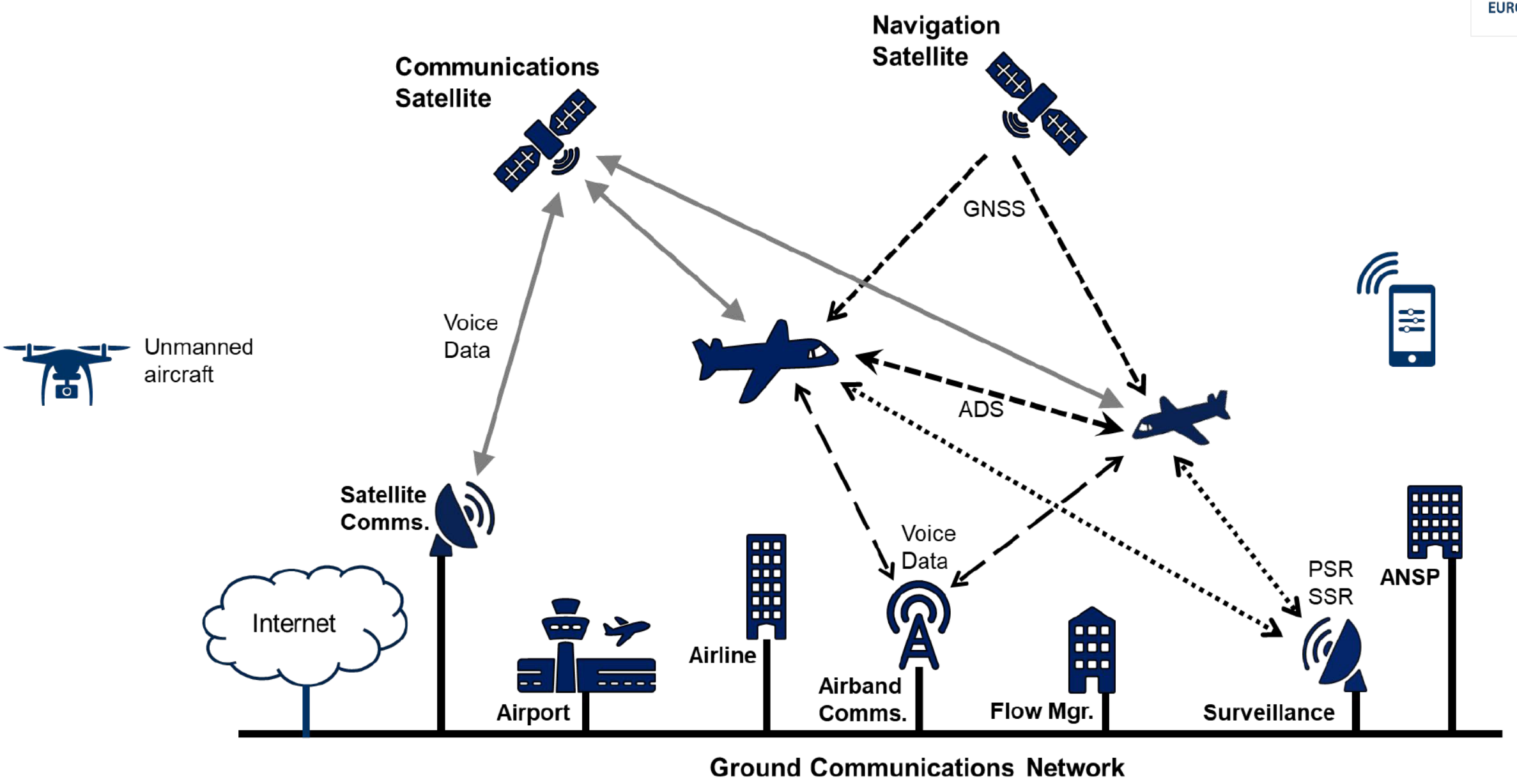
Cel: Ochrona lotnictwa przed ryzykiem w zakresie bezpieczeństwa informacji, mogącym mieć wpływ na bezpieczeństwo lotnicze.

Zakres: Systemy teleinformatyczne i dane wykorzystywane przez Zatwierdzone Organizacje i właściwy organ do celów lotnictwa cywilnego.

Działania:

- identyfikowanie ryzyka w zakresie bezpieczeństwa informacji związanego z systemami teleinformatycznymi i danymi wykorzystywanymi do celów lotnictwa cywilnego oraz zarządzanie tym ryzykiem;
- wykrywanie zdarzeń zagrażających bezpieczeństwu informacji, z identyfikacją tych, które są uznawane za incydenty bezpieczeństwa informacji;
- reagowanie na te incydenty bezpieczeństwa informacji i usuwanie ich skutków.

Aviation System



PART IS Information Security

Anneks II 2023/203	Anneks II 2022/1645	OPIS	NADZÓR
IS.I.OR.100	IS.D.OR.100	Zakres stosowania	IS.AR.100
IS.I.OR.200	IS.D.OR.200	System zarządzania bezpieczeństwem informacji (SZBI/ISMS)	IS.AR.200
IS.I.OR.205	IS.D.OR.205	Ocena ryzyka związanego z bezpieczeństwem informacji	IS.AR.205
IS.I.OR.210	IS.D.OR.210	Zmniejszanie ryzyka związanego z bezpieczeństwem informacji	IS.AR.210
IS.I.OR.215	IS.D.OR.215	System wewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji	
IS.I.OR.220	IS.D.OR.220	Incydenty związane z bezpieczeństwem informacji – wykrywanie, reagowanie i działania naprawcze	IS.AR.215
IS.I.OR.225	IS.D.OR.225	Reagowanie na niezgodności, o których powiadomił właściwy organ	
IS.I.OR.230	IS.D.OR.230	System zewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji	
IS.I.OR.235	IS.D.OR.235	Zlecanie czynności w zakresie zarządzania bezpieczeństwem informacji	IS.AR.220
IS.I.OR.240	IS.D.OR.240	Wymagania dotyczące personelu	IS.AR.225
IS.I.OR.245	IS.D.OR.245	Prowadzenie rejestrów	IS.AR.230
IS.I.OR.250	IS.D.OR.250	Podręcznik zarządzania bezpieczeństwem informacji	
IS.I.OR.255	IS.D.OR.255	Zmiany w systemie zarządzania bezpieczeństwem informacji	
IS.I.OR.260	IS.D.OR.260	Ciągłe doskonalenie	IS.AR.235

Przykłady zagrożeń i łagodzenie ryzyka

Zagrożenie	Opis	Przykłady łagodzenia ryzyka
Nieautoryzowany dostęp	Dostęp do systemów lub danych przez osoby nieupoważnione.	* Silne uwierzytelnianie *uwierzytelnianie wieloskładnikowe (MFA, 2FA) * Listy kontroli dostępu * Zasada minimalnych uprawnień
Naruszenia danych	Ujawnienie wrażliwych informacji.	* Szyfrowanie danych podczas przesyłania i przechowywania * Środki zapobiegania utracie danych (DLP, IDS, IPS, SIEM)
Ataki złośliwego oprogramowania	Wprowadzenie złośliwego oprogramowania (np. wirusów, oprogramowania ransomware) do systemów.	* Oprogramowanie antymalerowe * Regularne aktualizacje i łatanie oprogramowania * sandbox
Ataki typu „odmowa usługi” (DoS)	Przeciążenie systemów, aby uczynić je niedostępnymi.	* firewalls * IDS * CDN*systemy anty DDoS
Ataki typu „Men in the middle” M-I-T-M	Przechwytywanie i manipulowanie danymi podczas przesyłania.	* Szyfrowanie (np. TLS/SSL) * Bezpieczne protokoły sieciowe
Zagrożenia wewnętrzne	Zagrożenia pochodzące z wewnątrz organizacji (np. niezadowoleni pracownicy).	* Sprawdzanie przeszłości pracowników * Monitorowanie aktywności pracowników * Zasada minimalnych uprawnień*SZKOLENIA -Awerness
Ataki na łańcuch dostaw	Kompromitacja systemu poprzez lukę w produkcie lub usłudze dostawcy.	* Ocena ryzyka dostawców * Bezpieczne praktyki rozwoju oprogramowania * Sprawdzanie integralności oprogramowania

ISO/IEC 27000 family

- **Zbiór norm:** Seria międzynarodowych standardów, które pomagają organizacjom zarządzać bezpieczeństwem aktywów informacyjnych.

- **ISO/IEC 27001:** Najważniejsza norma z rodziny, określa wymagania dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

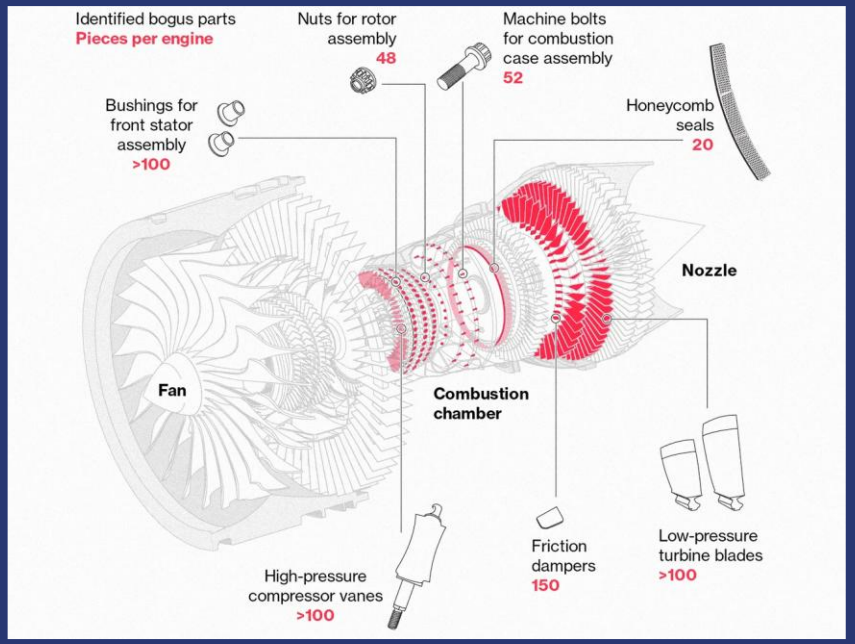
- **Inne normy:** Rodzina obejmuje również inne normy, które dostarczają wytycznych i najlepszych praktyk w różnych aspektach bezpieczeństwa informacji (np. zarządzanie ryzykiem, audytowanie, bezpieczeństwo sieci).

- **Podejście procesowe:** Normy z rodziny ISO 27000 promują podejście procesowe do zarządzania bezpieczeństwem informacji.

- **Zastosowanie:** Mogą być stosowane przez organizacje dowolnej wielkości i branży, w tym w lotnictwie.

Ponadto, mapowanie głównych zadań wymaganych w ramach Part-IS oraz klauzul i powiązanych kontroli w ISO/IEC 27001 znajduje się w Dodatku II opublikowanych Akceptowalnych Sposobów Spełnienia i Materiałów Doradczych (AMC & GM) do Part-IS.

Podrabiane części zamienne – AOG Technics, tuleje CFM56, sfałszowana dokumentacja.



- AOG Technics Ltd. – brytyjski dystrybutor części lotniczych.
- Dystrybucja niezatwierdzonych części do silników (głównie CFM56, ale też CF6) wraz ze **sfałszowanymi certyfikatami zdatności do lotu** (np. EASA Form 1, FAA 8130-3).
- *Przykład:* Tuleje (bushings)
- Zgłoszenia od organizacji MRO (np. TAP Maintenance & Engineering) do producentów (Safran, GE) i władz lotniczych (EASA, UK CAA, FAA) w 2023 r.
- **Skutki:**
  - Globalne dochodzenie i inspekcje.
  - Uziemienia samolotów, pilne wymiany części.
  - Znaczne koszty operacyjne dla linii lotniczych.
  - Poważne zagrożenie bezpieczeństwa lotniczego.
  - Podważenie zaufania do łańcucha dostaw.
- Krytyczna potrzeba weryfikacji dostawców i dokumentacji, czujność w całym łańcuchu dostaw.

Podsumowanie

Kluczowe Informacje do Zapamiętania

CO? Nowe przepisy **Part-IS** dotyczące bezpieczeństwa informacji.

KTO? Prawie wszystkie organizacje w lotnictwie cywilnym (CAMO, 145, ATO, etc.).

KIEDY? Pełna zgodność wymagana od **22 lutego 2026 r.**
DOA, POA, Lotniska – 16 października 2025 r

JAK? Poprzez wdrożenie **Systemu Zarządzania Bezpieczeństwem**

Informacji (ISMS) opartego na ryzyku.

PAMIĘTAJ: Bezpieczeństwo informacji to teraz integralna część bezpieczeństwa lotniczego.

Urząd Lotnictwa Cywilnego

DZIĘKUJĘ ZA UWAGĘ

Aldona Spirzewska

LTT-2

(Specjalista, Tel: +48 734 118 963
aspirzewska@ulc.gov.pl)

2.09.2025