EUROCAE ED-206 ISMS Reporting Considerations

Under **EUROCAE ED-206**, particularly in the context of **Chapter 6.4.3 – Security Event Reporting**, the document outlines **reporting timeframes and criteria** for **internal escalation** and **external notification**, aligned with aviation regulatory expectations (including those from EASA and ICAO). While ED-206 itself is guidance (non-binding), it is designed to support compliance with mandatory rules like **EASA Part-IS** and **EU Regulation 2023/203**.

Security Event Reporting – Timeframes & Criteria (ED-206 Context)

1. Reporting Timeframes

While ED-206 itself **does not specify exact hours** (unlike regulations), it references **urgency levels** and promotes alignment with **organizational policies and regulatory obligations**, such as:

- **Immediate (within 2 hours):** For severe or safety-affecting cyber incidents (e.g., potential loss of separation, communication failure, critical ground or airborne system compromise).
- **Short-term (within 24 hours):** For moderate impact events that may escalate or require external coordination.
- **Routine (within 72 hours):** For low-impact anomalies or when required for compliance.

ED-206 recommends that **timeframes be defined in the internal procedures** and harmonized with national or international regulatory reporting frameworks (e.g., **EU 2023/203**, **ICAO Annex 17/19**, or **EASA Part-IS AMC/GM**).

2. Criteria for Reporting Events

Events should be reported based on **impact severity, potential to escalate, and regulatory relevance**. The guidance outlines multiple **triggers** for reporting:

a. Technical Triggers

- Unauthorized access to systems or networks (attempted or successful)
- Detection of malware or malicious code
- Loss of confidentiality, integrity, or availability of systems supporting safety-critical operations
- Security anomalies affecting CNS/ATM, navigation databases, or flight operations

b. Operational Triggers

- Events impacting **safety of flight**
- Loss or degradation of air-ground communications, surveillance systems, or control infrastructure
- Disruption of flight planning, passenger data, or crew scheduling systems

c. Compliance Triggers

- Any event classified as a **"significant cyber event"** under **EASA IS.D.OR.205 / IS.A.OR.205** or **EU 2023/203**, requiring **notification to competent authorities**
- Breach of **GDPR**, **data protection laws**, or internal security policies
- Event that may require **coordinated response** with **NIS authorities, CSIRTs**, or aviation security partners

ED-206 Reporting Levels (Aligned with EASA/EU Framework)

Level	Description	Suggested Reporting Timeframe
Level 1 – Critical	Event affects flight safety or critical ground systems	**Immediately (≤ 2 hours)**
Level 2 – Major	Significant disruption or threat of escalation	**Within 24 hours**
Level 3 – Moderate	Event has contained impact; still requires analysis/logging	**Within 72 hours**
Level 4 – Minor	No impact or threat; reported for completeness or trend data	**As per internal schedule**

Internal vs External Reporting

- **Internal Reporting:** Should follow the incident response plan and **report to the SEM function** or designated cybersecurity lead immediately upon detection.
- **External Reporting:** To **competent authority (e.g., NAA, EASA, CSIRT)** based on the defined **urgency level and regulatory requirement**.

EU Regulation 2023/203, **IS.D.OR.205**, and associated AMC/GM clarify that **significant events** must be reported **"without undue delay and, in any case, within 72 hours."**

Summary

- **Timeframes:** Typically range from **immediate to 72 hours** based on severity.
- **Criteria:** Include any event with impact on **safety, operations, compliance**, or **cyber resilience**.
- **Guidance:** ED-206 recommends reporting policies be tailored but aligned with **EASA and ICAO expectations**, emphasizing **timely internal escalation** and **structured external coordination**.