POSITION PAPER

Reporting of Aviation Security Occurrences and Incidents

1. In March 2022, the ICAO AVSEC Panel endorsed new guidance material on the Reporting of Aviation Security Occurrences and Incidents that was developed in coordination with the ICAO Secretariat and relevant working groups of experts, then endorsed by the ICAO Aviation Security Panel.

2. From June 2022, the new ICAO Incident Reporting Guidance and Taxonomy remains publicly available in the six ICAO languages and is intended to assist States and industry stakeholders in the implementation of harmonized reporting processes for aviation security occurrences and incidents, based on a common taxonomy.

3. IATA actively participated in the development of the ICAO guidance and fully supports ICAO guidance and its clear and harmonized taxonomy for reporting security occurrences and security incidents aimed at facilitating analysis, information sharing and overall proactive efforts for improving the system. The taxonomy is fully aligned with IATA taxonomies.

4. In December 2024, IATA published an initial Position Paper on Security Incident Reporting on the public Security website outlining the legal background for security incident reporting in both ICAO Annex 17 for States and the IATA Operational Safety Audit (IOSA) Standards Manual (ISM) for airlines, including the new guidance on the ICAO website and IATA SeMS Manual.

Security Occurrence versus Security Incident

5. The ICAO guidance proposes a definition for security occurrence and security incident respectively:

    a. **Security Occurrence**: Any security-related event that may result in a reduced security outcome, may increase the operational risks or endangers the safety of passengers, crew, ground personnel and the general public, or is a potential compliance breach. This includes the identification or observation of a vulnerability in the protection of civil aviation against acts of unlawful interference

    b. **Security Incident**: A designation given to a security occurrence which affects or could affect the safety of passengers, crew, ground personnel and the general public. Security incidents are designated by a security official or manager to a reported security occurrence based on an analysis of the occurrence and a determination that additional action is required. A security incident may also result in an act of unlawful interference that would require additional reporting to ICAO (Annex 17 Standard 5.3.1 and Appendix 42 to the ICAO Aviation Security Manual refer).

6. The guidance further develops reporting processes for occurrences and incidents, including the expected report contents, mandatory versus voluntary reporting, and the analysis for occurrences and incidents. It also proposes a categorization of security incidents into levels of severity for assigning different reporting timeline requirements and finally shares a clear and harmonized taxonomy aimed at facilitating analysis and information sharing.

Reporting of Acts of Unlawful Interference

7. According to the last sentence in the ICAO definition of security incident, some security incidents may also result in being designated as "acts of unlawful interference" by the State(s) concerned, but their official notification would require additional reporting to ICAO following a template available in the ICAO Aviation Security Manual (Appendix 42), according to an Annex 17 provision (Standard 5.3.1, 2022). In this context, individuals, entities and organizations could report occurrences and incidents directly to their appropriate authorities, but only these appropriate authorities could report an act of unlawful interference to ICAO.

8. Some occurrences reported as hijacking, hostage situation, attack on the ground or bomb threat should be reported by States as "acts of unlawful interference" due to the direct alignment with the Annex 17 definition. Such occurrences should immediately be reported as an incident, so that State(s) could conduct proper criminal and technical investigations (including per Annex 13). State(s) should then share preliminary report(s) to ICAO as soon as practicable after the act is resolved (Annex 17 Standard 5.3.1) and then final report(s) according to the Appendix 42 of the ICAO Aviation Security Manual (Doc 8973, Restricted). The final report(s) on an act of unlawful interference issued by the State(s) concerned and shared with ICAO on a confidential basis, is/are usually produced many months after the occurrence took place, after all national, and sometimes international (as per Annex 13) investigations are concluded.

Reporting of Security Occurrences

9. Security occurrences could be reported by a large variety of individuals ranging from passengers, crew, ground staff, to the general public. Such reporting could be performed via different means of communication such as direct messages (email, or equivalent), direct oral reporting (at information desks), phone hotlines, via websites with or without dedicated reporting pages, and internal reporting systems (usually the case for aviation operators and entities).

10. Individuals other than staff from an aviation entity will probably report directly to authorities (aviation, police, customs, etc.) or at airport information desks.

11. Staff from aviation entities will probably report via the internal reporting system of the entity they are working for. Some staff could also report occurrences directly to the authorities, sometimes to the press.

Analysis of Security Occurrences

12. All security occurrences should be analyzed by designated security officers, security managers, or security analysts of the receiving entities to determine whether additional actions may be required.

    a. Determination is usually achieved by taking a prima facie approach to establishing whether the mixture of human factors is involved and/or evidence of a more systemic vulnerability in the way measures and controls are applied to prevent occurrences.

    b. If the prime facie analysis is benign, meaning that no investigation into the occurrence is warranted based on organization thresholds, then the occurrence is appropriately categorized as per established taxonomy for statistical purposes.

    c. Good security culture recommends that the staff having reported the occurrence should be provided with some feedback.

    d. If the prima facie analysis reveals unacceptable aspects, the occurrence reported should be elevated to the status of security incident, from which further investigation is required. This may include mandatory reporting of the security incident to the authorities according to relevant NCASPs, as well as further impact risk assessments for assessing if remedial actions are required.

Coordination between External Service Providers (ESPs) and Operators

13. As the outsourcing of the implementation of security measures from Operators to ESPs does not transfer the official responsibility for the reporting of security incidents, all security occurrences reported to and by External Service Providers (ESPs) should be shared with the respective entity who contracted the services (the Operator). The same coordination should apply when ESPs decide to report security incidents directly to the authorities as the potential consequences for their clients, the Operators, must be considered.

14. Conditions of the quality oversight functions performed by ESPs, including the identification and correction of deficiencies, as well as the obligation to report occurrences and incidents are typically covered in the IATA Standard Ground Handling Agreement (SGHA) and in the ISM.

Reporting of Security Incidents

15. When security occurrences are formally elevated to security incidents after the proper analysis (investigation, confirmation) by designated security officers, security managers, or security analysts, the entities should officially report the security incidents to their appropriate authorities (Annex 17 Standard 5.1.6 and ICAO guidance material, section C).

16. The report for security incidents should be formatted following the ICAO guidance, including the use of the harmonized taxonomy, for facilitating further analysis and information sharing.

Risk Assessments of Security Incidents

17. When an occurrence is elevated to the level of security incident, it means that a breach, or a vulnerability in the existing system has been identified (occurrence) and confirmed (incident). This is often termed "realized risk" meaning that something wrong happened that could have been exploited for endangering the protection of civil aviation and the safety of passengers, crew, ground personnel or the general public.

18. Operators and entities having adopted a Security Management System (SeMS) may consider a range of quality assurance functions such as perform a root cause analysis, conduct a security risk assessment, exercise to determine all corrective actions necessary for mitigating the new identified risks, or required for regulatory compliance purposes.

19. When all remedial and corrective actions could be directly implemented by the SeMS Operator or SeMS entity or their respective ESPs, then proper monitoring should be performed to ensure effectiveness in preventing future incidents or occurrences.

20. When all remedial and corrective actions have been effectively implemented, and the situation resolved, then the incident should be closed, and its closure reported to the authorities (together with the list of remedial and corrective actions taken). Where necessary, corrective action should be verified at future intervals to ensure ongoing and effective implementation.

Severity Assessments of Security Incidents

21. When the assessment performed by the Operators or entities reveals more serious potential impacts on the general security level of the system, or when the necessary remedial corrective actions could not be implemented by the Operator or entity in isolation, then another report should be provided to the authorities

highlighting the assessment of the severity or seriousness of the incident, as well as the limited corrective actions available at the Operator or entity level.

22. These security incidents categorized with a high level of severity could be named "potentially serious security incident", or using any other denomination, but their additional reporting could only take place after a proper risk assessment has been completed, which may require the involvement of other partners (such as law enforcement agencies) meaning delays that are not under the control of the reporting entity.

Reporting timelines for Security Incidents

23. As indicated in the ICAO guidance, reporting timelines should only apply to security incidents (not security occurrences) and to the Operators and entities reporting incidents to their appropriate authorities.

24. Note the time and date of an occurrence may be different than the time and date the occurrence was reported to a qualified security professional. The same applies to the difference between the time and date of an occurrence and when the occurrence may have been elevated to an incident.

25. The guidance proposes "not later than 48 hours", "not later than 72 hours" and "on monthly basis" but unfortunately without specifying the starting date of the timeline? The date of reception of the original occurrence report? The date of completion of the analysis of the occurrence report elevating this occurrence to the status of incident? The date of completion of the full risk assessment of the incident for evaluating its severity?

26. An automatic reporting of all security incidents to the authorities could be counterproductive (and resource intensive) as most of the minor incidents (of operational nature, such as minor noncompliance) are resolved directly by the Operators, entities and their ESPs as part of their Security Management System (SeMS).

27. As explained in the "Reporting Acts of Unlawful Interference" section, when an occurrence is obviously linked to the Annex 17 definition of acts of unlawful interference, this occurrence should be immediately elevated to a security incident, and immediately reported to the appropriate authorities, Appropriate and relevant authorities could further progress on the investigation and official ICAO reporting sides. The Operator's risk assessment of the incident should continue in parallel with the immediate reporting.

28. The reporting of all closed security incidents, together with their resolution, could be more useful for data analysis and performance indicator purposes. The timelines for reporting closed security incidents could be fixed based on the date of elevation from an occurrence to an incident, meaning when internal remedial and corrective actions are taken, not on a fixed day in the calendar (such as each end of the month).

29. When the assessment of one security incident reveals the potential for a high level of severity with potential serious impacts on the general security level, or the operability of the system, these "potentially serious security incidents" could be immediately reported to the authorities, together with the outcome of the internal risk assessment categorizing such incident at high level of severity.

30. However, fixing artificial deadlines for reporting such "potentially serious security incidents" to appropriate authorities is unrealistic when considering the time and resources necessary for performing proper risk assessments of the incident and its potential severity.

31. Finally, as stated in the background section of the first IATA Security Incident Reporting (Dec 2024) Position Paper, the ICAO Incident Reporting Guidance and Taxonomy is fully aligned with the IATA harmonized security taxonomy promoted in the SeMS program and the SeMS Manual, as well as the IATA Incident Data eXchange (IDX) safety and security incident data management program. All IOSA registered airlines are invited to report safety and security occurrences and incidents via IDX (ISM ORG, GRH and SEC Sections).

For any questions, please contact aviationsecurity@iata.org