Reporting of Aviation Security Occurrences and Incidents

NOTE.— Developed in coordination with the Secretariat and relevant Working Groups of experts, this guidance material was endorsed by the Aviation Security Panel at its Thirty-third meeting, which recommended that it be made available as soon as practicable. It will also be included in the forthcoming 13th edition of the ICAO *Aviation Security Manual* (Doc 8973 – Restricted).

Published by authority of the Secretary General

June 2022

International Civil Aviation Organization

GUIDANCE MATERIAL FOR REPORTING OF AVIATION SECURITY OCCURRENCES AND INCIDENTS

Contents

Definitions

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.

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 5.3.2 and Appendix 42 to the ICAO *Aviation Security Manual* refer*).*

General

Reporting of security occurrences by individuals, entities and organizations in the aviation system is necessary to collect information that may be analyzed by a security official or manager as precursors for security incidents, or preparatory acts of unlawful interference, leading to:

- Identifying threats and vulnerabilities in the aviation security system;
- Informing the entity to update their risk assessment and changes thereto;
- Informing location specific and national risk assessment and changes thereto;
- Monitoring of trends and patterns in aviation security;
- Analyzing root causes and causal/contributing factors of security occurrences or incidents;
- Reinforcing relevant information sharing between authorities and industry stakeholders for enhancing respective risk assessments; and
- Bolstering the security culture among all aviation stakeholders.

Reporting should be performed in a structured and harmonized manner with processes developed and/or required by the appropriate authority and clearly defined in the National Civil Aviation Security Programmes. Doing so will ensure practical and timely reporting to the relevant authorities, taking into account protection of sensitive aviation security information.

In order to encourage the open and transparent reporting of security occurrences from all entities, it is important that the appropriate authorities refrain from issuing findings and taking other regulatory action until after official oversight activities are completed (i.e. investigation and analysis).

Global harmonization of aviation security reporting processes could improve consistency for industry stakeholders in submitting reports to different national authorities. Harmonization could also create opportunities for sub-regional, regional and international analysis of security incidents based on interlinked taxonomies.

This guidance is intended to assist all stakeholders in the aviation security environment to develop, implement and maintain an effective and efficient reporting system for security occurrences and incidents. This guidance takes into account existing reporting systems, to include those used in the safety environment, “Just Culture”, and reporting of unruly and disruptive passengers (more information can be found in Chapter 9 and Chapter 16 of the ICAO *Aviation Security Manual*, respectively).

Security Occurrences and Security Incidents

Events and activities that appear to be abnormal, unusual, strange, etc. should be reported internally or directly to authorities through appropriate channels by any person. This is the example of a witness informing airport staff or the police about the piece of luggage left unaccompanied in public area. This could also be the case of an access door kept open when it should be securely closed. If that observation, impression, feeling, or activity is not reported, then it is lost even if it could have been a good indicator or precursor for security analysts.

Security incidents are security occurrences reported by staff, crew, ground personnel, subcontractors, media, the public and/or passengers that are analyzed by a security subject matter expert, for example the security official or manager of the entity who received report, or the authorities in case of direct reporting. A security incident is potentially threatening and could lead to harming the public, staff, and/or crew, to disruption of service, to loss of reputation, and should always be taken seriously.

Security Occurrence Reporting Process and Timeline

The reporting process of security occurrences should take into account the following elements:

- Security occurrences can be reported by staff, crew, ground personnel, the public and/or passengers, regardless of whether or not they are fully trained to identify security precursors or nuances;
- The instructions and tools for reporting security occurrences should be simple and accessible to all;
- Reporting security occurrences within an entity or an organization could be an internal mandatory process for all staff (implemented by virtue of internal quality control, Security Management Systems, etc.). In that case, the reporting of security occurrences is performed by the staff to its designated security official or manager as per internal procedures;
- Security occurrences could also be reported directly to authorities via dedicated interfaces;
- All security occurrences reported should be analyzed by an appropriate security official or manager to determine if it rises to the level of a security incident, and to ensure corrective action(s) are taken if/when necessary; and
- A log of security occurrences reports should be maintained together with the action(s) taken.

As time could be of the essence, all security occurrences should be reported as soon as possible, and ideally the same day of the occurrence, keeping in mind that individuals reporting an occurrence may need time to process what they have observed.

Security Occurrence Reporting Content

As the content of occurrence reporting should help in constructing the official incident report, it is advisable that existing occurrence reporting systems (by entities, operators, etc.) may be adjusted to contain at least the following elements:

- Location of the occurrence, using if possible official designation;
- Exact date and time of the occurrence;
- Description of the occurrence as precise as possible;
- Name of the person reporting (if possible); and
- Immediate action(s) taken upon the identification of the security occurrence, such as notifying local law enforcement and/or airport authorities of the situation.

Analysis is an essential step in the process of dealing with an occurrence. In general, it should consist of a factual description of the reported event and an interpretation of the facts. In any case, it should be proportionate to the level of risk associated with the event. Thus, for the least significant occurrences, the analysis may be reduced to a simple evaluation and a closure without follow-up. Conversely, the most significant occurrences will be analyzed in depth.

Security Incident Reporting Process and Timeline

When a security occurrence has been designated a security incident, several actions need to take place:

1. Immediate corrective actions should be taken to address vulnerabilities identified in the report;
2. The information contained in the security occurrence report, together with the analysis and corrective actions initiated by the security official or manager, should be compiled into a security incident report to be shared with the appropriate authorities; and
3. All reports and actions should be recorded for quality control and auditing purposes.

The reporting of security incidents to the appropriate authorities should be performed as soon as possible after an occurrence is designated as an incident. Doing so will help facilitate timely corrective actions and/or the further sharing of information, as appropriate, to address vulnerabilities.

The immediate reporting of security incidents to the appropriate authorities is also essential in the event other security incidents are occurring locally, nationally or internationally, that are linked and/or are indicators that a security threat is evolving. Nonetheless, some reporting systems may categorize security incidents into levels of severity and assign different reporting timeline requirements. Figure-001 provides an example as to how a State might define which incidents should be reported within a particular timeframe with a particular mean.

Type of incident	Notification by telephone	Written report
TBD	Immediate	No later than 48 h
TBD	-	No later than 72 h
TBD	-	On monthly basis

Figure-001

Security Incident Reporting Content

The following elements should be considered the minimum information to be included in a security incident report, to allow for a structured and harmonized collection of relevant data:

- Location of the occurrence as originally reported;
- Adjusted location if required (official designation after the analysis);
- Date and time of the occurrence as originally reported;
- Description of the occurrence as originally reported;
- Additional description information (after the analysis);
- Type/class/category according to established taxonomy (after the analysis);
- Entity providing the incident report (and name of the security official or manager completing the report);
- Immediate actions taken following the report of the occurrence and the classification as security incident;

- Plan of remedial or additional actions required; and
- Estimated consequences and perceived severity of the incident (by the security official or manager).

Mandatory versus Voluntary Reporting

Reporting systems should facilitate processes for submitting reports, analyzing data, and generating relevant security information. An overly complex system may discourage reporting or result in inaccurate reporting; therefore the system should be designed to promote positive reporting cultures with ease of use in mind. The system should capture all relevant information about an occurrence, including what happened, where, when, and to whom the report is intended.

States are required to define processes for the reporting of information concerning aviation security incidents to the relevant national authorities by any entity responsible for the implementation of the National Civil Aviation Security Programme, as illustrated in Figure-002.

States should supplement their national civil aviation security quality control programme by establishing a confidential reporting system for analyzing security information provided by sources such as passengers, crew and ground personnel as per Annex 17 requirements and in [7.2.8] “Gathering of information from outside sources”.

Aviation security reporting systems (as a part of “Security Culture” processes) are outlined in Chapter 9 of the ICAO *Aviation Security Manual)*.

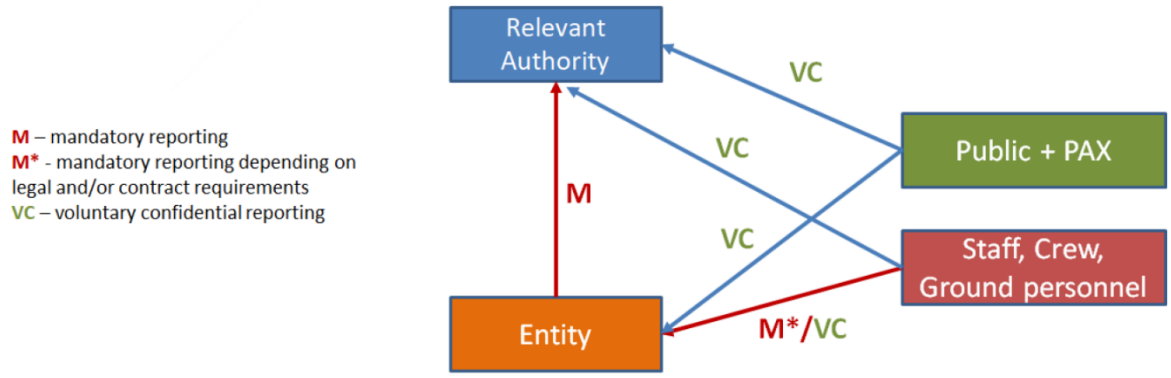

Figure-002

Reporting Methods

Different methods of reporting may be established, depending on notification timeframes and practices in the State concerned. Options could be a dedicated telephone number, fax number or e-mail address, a written report, or an interactive platform such as a website or app. Reporting may be required in a defined format with mandatory fields. Advantages of such a form would be the facilitation of a rapid response and consistency of data. If necessary, a classification of confidentiality should be included in the form. The confidentiality aspect may also influence the decision on how certain information can be submitted.

Incident Report Analysis

An efficient and effective aviation security incident reporting system should enable States to:

1. Respond promptly and effectively to incidents;
2. Help inform considerations about the effectiveness of:
    a. current processes and procedures;
    b. training; and
    c. equipment, etc.;
3. Identify trends or patterns which can help inform policymaking;
4. Identify gaps in current regulations and national programmes;
5. Define priorities in policy;
6. Establish updates of aviation security measures, including policy changes, where necessary;
7. Share relevant information with other States and entities as appropriate;
8. Initiate appropriate investigation;
9. Manage public concern or media interest in incidents; and
10. Assess the significance of an incident or incidents when combined with intelligence or other information held by government.

Assessment of Aviation Security Incident Information

States should establish and maintain a process to assess and analyze the information contained in security incident reports that lead to identification of threats and vulnerabilities in the aviation security system. This will enable States to undertake risk assessment and formulate mitigating measures, as well as root cause analysis, identify contributing factors and monitor trends and patterns in aviation security.

States should have processes in place to measure the effectiveness of current security procedures. These processes enable States to identify and close gaps in current regulations and national programmes. States will be able to define priorities in policy as well as establish updates of aviation security measures, which may include a change in policy, where applicable. States will be able to initiate appropriate investigation, and will be able to share relevant information with other States and entities as deemed necessary.

States and stakeholders should establish, implement and maintain procedures outlining threat and risk assessment roles and responsibilities in order to be capable of addressing any immediate threats to aviation security.

Protection of the Information

Some, if not all, information in security occurrence and incident reports may need to be handled as sensitive aviation security information, including the identity of the authors.

Security data and information contained in security reports should be shared on a need-to-know basis and for the purposes of addressing vulnerabilities and enhancement of the aviation security system. More information on sensitive aviation security information can be found in Chapter 2 of the ICAO *Aviation Security Manual* (Doc 8973 — Restricted).

Training and Awareness

Training, awareness actions and security culture are critical for an effective implementation of any reporting system of security occurrences and security incidents.

A lack of understanding of the purpose and utility of security occurrence and incident reporting can result in serious vulnerabilities remaining unrevealed to concerned operators, authorities, and entities. Staff, stakeholder and public engagement, as well as the integration of a reporting culture in daily activities, is essential for the collective success and protection of the ecosystem.

Training of managers and supervisors for the purpose and value of security occurrence reporting and incident reporting as a continuous risk management and Security Management System performance tool is fundamental to maintaining a healthy aviation security ecosystem.

When conducting exercises, the security occurrence and incident reporting process should be tested and practiced. This gives the opportunity to identify issues with the process in a non-urgent matter while also increasing familiarization with roles and responsibilities.

Given that there could exist several different legislative requirements linked to security occurrence and incident reporting, States could consider providing a consolidated best practice document that outlines key requirements and procedures to provide stakeholders a clear understanding of what is expected.

Several training tools and programmes on security occurrence and incident reporting are available through ICAO, States, organizations, and industry stakeholders. All entities who operate within the aviation ecosystem should be encouraged to undertake initial and recurrent training on security occurrence and incident reporting for their job function. This could also be a required competency in order to maintain job certification, where applicable.

Public campaigns that use posters, videos and/or social media can be a useful tool to educate and encourage security occurrences reporting from the general public as well as those who work in the aviation environment. Examples of such public campaigns can be found on the ICAO Security Culture website[1].

Taxonomy

The establishment of a clear taxonomy and harmonized procedure for reporting of aviation security occurrences and incidents, together with development of a global and harmonized secure tool for reporting, would further encourage the aviation security incident reporting process and increase the probability of reporting of security incidents affecting civil aviation, which will result in the development of a strong security culture.

Security data should ideally be categorized using taxonomies and supporting definitions so that the data can be captured and stored using meaningful terms. Common taxonomies and definitions establish a standard language, improving the quality of information and communication.

The main focus of these guidelines is on harmonizing security incident reporting taxonomy, which aims to facilitate analysis and information sharing, and exchange between the State and industry stakeholders (in particular the aircraft operators). Noting that many States and a few civil aviation organizations have already developed robust safety and security taxonomies used by subject matter experts for reporting (safety and) security incidents to their authorities and industry peers, further work on harmonization of models between security and safety may be required. Therefore, States are strongly encouraged to agree and coordinate implementation of taxonomies as well as reporting templates and timelines with industry stakeholders.

In light of the above, the following taxonomy has been developed to assist States and stakeholders in implementing a harmonized reporting system for aviation security occurrences and incidents.

[1] https://www.icao.int/Security/Security-Culture/Pages/default.aspx

Security Incident Taxonomy

Class*	Category**
Landside security	Discovery or use of vehicle-borne improvised explosive device (IED)
	Discovery or use of person-delivered IED
	Armed attack
	Unattended/suspicious items (also applicable airside)
	Chemical, biological and radiological (CBR) attack
	Damage to critical infrastructure/vulnerable points
	Suspicious behaviour
	Unplanned disruptions, including bomb threat or hoax
Passengers and cabin baggage	Discovery or use of prohibited item/IED
	Deficiency in the security checkpoint screening process
	Mixing of screened and unscreened passengers
	Suspicious behaviour
Staff and crew	Deficiency in the security checkpoint screening process
	Discovery or use of prohibited item/IED
	Sabotage
	Insider bypassing security controls
	Deliberate attempt to circumvent vetting/background check regime
Access control	Breach or attempted breach of perimeter
	Unauthorized access to security restricted area (SRA) or other controlled area (non-staff)
	Unauthorized/unescorted access within SRA (staff)
	Suspicious behaviour of staff
	Deficiency in the access control system
	Deficiency in the ID pass issuing system
	Deficiency in the vehicle access control system including application of security controls and/or screening of occupants and vehicles
Hold baggage	Discovery or use of prohibited item/IED
	Deficiency in protecting screened hold baggage
	Evidence of tampering of screened hold baggage
	Deficiency in the hold baggage screening (HBS) system or process (including passenger baggage reconciliation)
	Deficiency in the process of transportation of dispatched weapons

Class*	Category**
In-flight supplies	Unauthorized access to in-flight supply facility
	Deficiency in protecting secure supplies
	Evidence of tampering of secured in flight supplies
	Deficiency in applying security controls
	Discovery or use of prohibited item/IED
Airport supplies	Unauthorized access to facility
	Deficiency in protecting secure supplies
	Evidence of tampering of secured airport supplies
	Deficiency in applying security controls
	Discovery or use of prohibited item/IED
Aircraft protection on the ground	Unauthorized passenger on the aircraft
	Unauthorized staff on the aircraft
	Deficiency in the aircraft security search/check
	Deficiency in aircraft protection measures, including where aircraft are parked overnight
	Discovery or use of prohibited item/IED in the aircraft cabin or hold
Aircraft in-flight security measures	Unruly passenger (to be considered for level 3 and 4 (see ICAO *Aviation Security Manual*) only to be reported)
	Deficiency in the cockpit door process/protection
	Discovery or use of prohibited item/IED
	CBR attack
	Hijacking in flight
	Bomb threat in flight
Cargo and mail	Unauthorized access to cargo screening facility
	Deficiency in the screening process
	Discovery or use of prohibited item/IED
	Deficiency in protecting secured cargo
	Evidence of tampering of secured cargo
	Deficiency in the acceptance process
	Suspicious activity
Air Traffic Control	Armed attack against air traffic control (ATC) facility
	Destruction or damage of air navigation aids
	Unauthorized access

Class*	Category**
Digital information and technologies	Attack against aircraft system(s)
	Attack against air traffic management (ATM) system(s)
	Attack against airport system(s)
	Attack against other critical systems and data
Unmanned aircraft systems (UAS) / Unmanned aerial vehicle (UAV) / Remotely-piloted aircraft system (RPAS)	Unauthorized incursion into controlled airspace
	Near miss/Encounter with aircraft in flight
	Strike/Collision with aircraft in flight
	Sighting from aircraft/airport
	Unmanned aerial vehicle (UAV) caused threat against aircraft
	UAV caused threat against airport infrastructure
	UAV caused threat against passengers
Stand-off weapon (MANPADs, etc.)	Attack on aircraft or airport facility
	Reported sighting
Lasers[2]	Attack on aircraft or airport facility
	Reported sighting
	Suspicious activity
Aviation security information	Deficiency in protecting sensitive aviation security information
	Loss of integrity and availability of information systems
General Aviation/Aeroclubs	Unauthorized access
	Discovery of prohibited item/IED

***Class:** describes the topic the security incident would refer to, such as 'access controls', 'hold baggage' or 'cargo/mail'. The chosen identifiers are already commonly used in ICAO Annex 17 and the *Aviation Security Manual*, and are expected to be easy for entities to refer to and relevant for authorities to make assessments.

****Category:** indicates a more specific description of the security incident involved. The categories differ per class as the possible security incidents vary depending on which aviation security process they relate to. For instance, the class 'aircraft protection on the ground' includes the category 'deficiency in the aircraft security search/check', whereas the class 'hold baggage' includes the category 'deficiency in protecting screened hold baggage'. There would also be a category 'other' for those incidents that may be too rare to justify a separate category or which may be considered a new threat or vulnerability. However, this option should only be used when none of the other categories seems suitable.

— END —

[2] Incidents involving the use of lasers may be reported as part of safety reporting programmes and safety management systems. It is therefore recommended that relevant national authorities provide clear guidance on how best to report such incidents.