International Civil Aviation Organization

WORKING PAPER

SECOND HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS/2)

Montréal, 29 to 30 November 2018

Agenda Item 2: Future approaches to managing aviation security risks

PROMOTING SECURITY CULTURE

(Presented by Belgium, Canada, Germany, Italy, New Zealand, Portugal, Qatar, Romania, Singapore, Switzerland, United Kingdom, United States and Airports Council International)

SUMMARY

Establishing a comprehensive security culture is imperative to long-term, effective aviation security. In alignment with the priority objectives of the Global Aviation Security Plan (GASeP), the ICAO Working Group on Training (WGT) of the Aviation Security Panel of Experts (AVSEC Panel), in collaboration with the ICAO Secretariat, is taking action to promote the importance of security culture and advance ICAO's ability to provide guidance and training to Member States on security culture.

Action by the High-level Conference on Aviation Security is in paragraph 4.

1. INTRODUCTION

1.1 Priority Outcome 2 of the ICAO Global Aviation Security Plan (GASeP) is focused on Developing Security Culture and Human Capability. Security culture is a set of norms, beliefs, values, attitudes and assumptions that are inherent to the daily operation of an organisation and are reflected by the actions and behaviours of all entities and personnel within the organization. In relating to aviation security, building a strong security culture will capitalize on shared resources, promote information sharing, ensure recognition that effective security is critical to business success, establish positive security practices among employees as a core value, and align security to core business goals. The WGT of the AVSEC Panel fully supports this key outcome and notes the importance of establishing and maintaining a strong and robust security culture alongside the development of human capital, skill and competency.

1.2 The WGT welcomes the following tasks under Priority Outcome 2 of the GASeP:

2.A Review or develop training material to teach security culture and its principles.

2.B Develop security awareness programmes that effectively promote a positive security culture.

2.C Continuous promotion of security awareness campaigns.

2.E Develop and disseminate to all other stakeholders communication plans, reporting tools, promotional materials and model training.

2.F Develop communication strategies to build the general public's awareness of aviation security and the importance of complying with security measures.

2. ACTIONS TAKEN BY THE WGT TO PROMOTE SECURITY CULTURE

2.1 The WGT, under its formal work programme and in collaboration with the ICAO Secretariat, has undertaken work to achieve the tasks outlined in the GASeP regarding security culture. In 2017, the WGT produced a Toolkit on Enhancing Security Culture (Appendix A), which is designed to assist organisations operating in the aviation industry to enhance a strong security culture for an effective security regime. The toolkit outlines a number of tools to support trainers and managers with embedding and sustaining strong security behaviours within the workforce.

2.2 The WGT have also been developing a Workshop on Enhancing a Positive Security Culture. The Workshop will be focused on senior and middle managers from industry and other persons responsible for the implementation of security measures, with the objective of assisting them to establish a positive security culture and improve their overall security performance through the early identification of potential security challenges. An outline for the Workshop was finalised at the WGT meeting in July of 2018.

2.3 In its efforts to promote security culture awareness, the WGT, in partnership with the ICAO Secretariat, developed a Security Culture Seminar as part of the activities of the 2018 ICAO Aviation Security Symposium. This Seminar provided participants with best practices to develop behaviour change campaigns and tools to implement a positive security culture within their organisation.

3. ENHANCING A POSITIVE SECURITY CULTURE

3.1 An effective security culture can result in employees who are engaged with, and take responsibility for, security issues. It is an essential component for a protective security regime, which supports and maintains a risk-resilient organization. Promoting a positive security culture helps to mitigate against both insider threats and external threats as personnel think and act in more security conscious ways and are able to identify and report behaviours or activities of concern. In turn, this results in all personnel feeling that they have a critical role to play within a security regime, and security overall being improved - for not just aviation security but for wider border security without the need for significant investment. From screeners to cleaners, and from taxi drivers to those working in airport retail outlets, all have a vital contribution to make to improve aviation security.

3.2 A robust and efficient security regime must be proactive and supported by competent people. Furthermore, a security culture can only be successful if people are accountable and motivated to follow established procedures, comply with prescribed regulation and take the initiative when unforeseen circumstances arise. An effective Security Management System (SeMS) can offer one way to achieve this by providing an organized, systematic approach to managing security which embeds security management and risk ownership into the day-to-day activities of the organization and its people.

3.3 The WGT recommends that all States, organisations and entities be encouraged to embrace and promote a positive security culture in order to deliver at an accelerated rate the applicable

GASeP Priority Outcome 2 actions. All should be encouraged to ensure capacity and capability are built up throughout the system by investing in human capital for a motivated and competent workforce. This will help to achieve a security culture where everyone knows their role and responsibilities within a security regime. Such actions could include those highlighted in Appendix A, the ***Security Culture Toolkit*¸** approved by the AVSEC Panel in 2018, which includes, but is not limited to: initial and recurrent training on security culture and continuous learning activities; promotion of security culture by senior leadership; a targeted communication plan and continuous security awareness campaigns; and the establishment of a reporting system that guarantees the confidentiality of reporting individuals.

3.4 The WGT acknowledges that a transformation in security culture behaviour and awareness can be challenging to deliver and to embed throughout an organisation from the top down. To receive the most benefit, States should take a multi-agency approach so that support for security culture is not just focused on aviation security but security as a whole. The WGT encourages States, organisations and industry to take immediate practical steps to begin delivering high profile behaviour change campaigns and other practical actions to promote a strong and sustainable security culture within their organisations.

4. ACTION BY THE HIGH-LEVEL CONFERENCE

4.1 The High-level Conference on Aviation Security is invited to:

a) Recognise the work done to date by the ICAO Working Group on Training and the AVSEC Panel to promote a positive security culture; and

b) Encourage States, organisations and industry to use the WGT security culture material to deliver immediate security improvements and longer term change by taking practical steps to enhance security culture within their respective jurisdictions or organisations.

— — — — — — — —

APPENDIX A

SECURITY CULTURE TOOLKIT

A priority action of the Global Aviation Security Plan (GASeP), as adopted by the Council of ICAO 10 November 2017, is to **Develop Security Culture and Human Capability**. This document produced by the ICAO Working Group on Training and endorsed by the ICAO Aviation Security Panel 19-23 March 2018 seeks to build and promote positive security culture by providing States and Industry with a toolkit of best practices.

Introduction

– What is Security Culture?

Security culture is a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of an organisation and are reflected by the actions and behaviours of all entities and personnel within the organisation. Security should be everyone's responsibility - from the ground up. Effective security culture is about:

- Recognising that effective security is critical to business success;
- Establishing an appreciation of positive security practices among employees;
- Aligning security to core business goals; and
- Articulating security as a core value rather than as an obligation or a burdensome expense.

Benefits

The benefits of an effective security culture include:

- Employees (staff) are engaged with, and take responsibility for, security issues;
- Levels of compliance with protective security measures increase;
- The risk of security incidents and breaches is reduced by employees thinking and acting in more security conscious ways;

- Employees are more likely to identify and report behaviours/activities of concern;
- Employees feel a greater sense of security; and
- Security is improved without the need for large expenditure.

Tools for the implementation of a positive security culture

This toolkit is designed to assist organisations operating in the aviation industry in enhancing their security culture. It outlines a number of tools to support trainers and managers with embedding and sustaining strong security behaviours within the workforce. The tools are grouped under the following intervention areas:

POSITIVE WORK ENVIRONMENT	
DESIRED OUTCOME	TOOLS
A work environment which drives and facilitates a positive security culture.	**Clear and consistent: policy, processes, systems and procedures –** enshrine security in all corporate policy and procedures, including those areas which do not have a primary security focus, such as the organisation's management plan. Document clearly in writing: policy, processes, systems and procedures which support a positive security culture. Ensure the information is easy to understand, simple to follow, and readily accessible to staff who may want to refresh their understanding.
	Equipment, space, resources – provide staff with the resources they need to achieve a strong security performance. This may be in the form of additional screening equipment, or by providing extra staff at a security checkpoint, or the provision of appropriate IT equipment or machinery.
	Prompts – help employees to implement good security by reminding them what actions they need to take. This could be notices on doorways reminding them not to allow tailgating (drive too closely behind another vehicle); or a pop-up prompt when logging on/off a computer.
	Suggestions box – allow staff the opportunity to suggest ways in which security could be improved. Reward suggestions which result in changes and improvements.
	Targeted communications plan - invite experts or celebrities from outside of the organisation to endorse security practices through fun messages. This could be via a video or an article or an in-person presentation.
Staff who know what security behaviours are expected of them and who confidently and willingly demonstrate the behaviours.	**Performance appraisals –** document for every employee what security behaviours are expected of them and assess their performance against these behaviours as part of the appraisal process. Provide feedback on their security behaviours, recognition for positive security behaviour, and consequences or sanctions for failure to adhere to security policy.
	Thank you messages - this may be in the form of a blog or an article on how strong security culture is impacting positively on the organisation. Or a corporate communication on the results of security checks e.g. 100% of employees were clearly displaying their security pass.
An organised, systematic approach to managing security which embeds security management into the day-to-day activities of the organisation and its people.	**Security Management System (SeMS) –** manage security in a structured way by implementing a SeMS. A SeMS can provide a risk-driven framework for integrating security into an organisation's daily operations and culture. The philosophy of SeMS is a top-to-bottom culture that leads to the efficient provision of a secure operation.

TRAINING	
DESIRED OUTCOME	TOOLS
Staff who have the knowledge, skills and capability to practice good security.	**Induction training** – equip employees with the knowledge, skills and abilities to practice good security from the outset. This includes those whose roles do not involve the implementation of aviation security measures. Educate new staff on the threat, in particular those who may pose a threat to civil aviation and their possible motives; the types of attack on aviation; and the reasons why aviation is an attractive target. Emphasise the importance of challenging non-compliance with security procedures/policy and include details of how to respond to security incidents. Provide examples of unusual/suspicious behaviour/items which should be reported. Use case studies, dummy items and role play to emphasise the message.
	Refresher training – provide refresher training at regular intervals so that employees can renew and update their knowledge of security matters. Training should include updates on emerging threats/recent incidents, security failures, suspicious behaviours and what to watch out for.
	Continuous learning activities – promote security messages throughout the year and support employees in expanding their security knowledge and skills. This may be in the form of security events, support with e-learning, and job shadowing or mentoring.
LEADERSHIP	
DESIRED OUTCOME	TOOLS
An environment where managers and leaders, including those at the highest level, lead by example and support their staff in implementing good security.	**Leadership briefings** - promote security messages through senior staff. Senior leaders could include security in part of their newsletters or staff briefings, or write an article or a blog on underlining the importance they place on good security and the actions they take personally to enhance and promote positive security culture.
	Example behaviour – support and personally apply security policy at all times and do not cut corners e.g. to save time.
	Patience and understanding - allow all staff the necessary time and resources to comply with security measures, even when under pressure.
	Thank you messages – personally thank those who have reported suspicious activity or security breaches.
	Involvement in security awareness events and staff briefings – senior management taking time to get personally involved in security awareness briefings and events. This would send a message to staff that managers/leaders have placed importance in security and are supportive for ongoing security initiatives.

UNDERSTANDING THE THREAT	
DESIRED OUTCOME	TOOLS
	Targeted threat briefings – provide middle and senior managers with targeted, more detailed threat briefings to maintain and enhance their understanding and appreciation of the threat.
All staff understand the nature of the threats they and their organisation face.	**Reminder briefings** – deliver regular reminders to existing staff and the wider airport community on security threats faced by the organisation. This could be via the intranet, in newsletters, at staff meetings, through annual refresher training or at specific coordinated briefing awareness sessions.
	Verbal updates when the threat picture changes – inform staff as soon as possible about new and emerging threats, or changes in threat level, and the implications of this for them and the organisation. This is best done face-to-face e.g. at staff meetings and shift briefings to allow staff to ask questions.
VIGILANCE	
DESIRED OUTCOME	TOOLS
All staff feel able to challenge those who are not complying with security policy /procedures.	**Repetition** – repeat messages for consistency and to help embed awareness. For example a person getting the same security messaging on recruitment, during induction, on pass issue, and throughout their employment.
	Reminder briefs - encourage staff to challenge non-compliance via briefings, handouts and posters in staff rest areas pointing out potential consequences of failing to challenge.
All staff and visitors pay attention to their surroundings when at the airport and know what unusual or suspicious behaviour looks like.	**Visitor briefing note -** create a short security briefing note to issue to all visitors along with visitors pass. The note could highlight the importance of paying attention to their surroundings when at the airport and provide contact details for the security room.
	Posters and signage – place signage around airport premises to remind staff and visitors to remain vigilant and pay attention to their surroundings. Contact details can be provided on the signage to advise the person who to contact if they detect suspicious personnel or activities.
	Regular security awareness campaigns – run security education campaigns at regular intervals to remind existing employees and airport operators about their role in protective security, what may constitute suspicious activity and the importance of reporting unusual behaviour or items. The campaign could include posters listing suspicious activities in staff rest areas, a blog or article on the intranet, including real-world examples or experiences, and a security awareness event showcasing protective security

	arrangements, with expert speakers, displays and presentations.
REPORTING SYSTEMS	
DESIRED OUTCOME	TOOLS
Security breaches and occurrences are reported swiftly and corrected. Staff do not feel as though they are 'telling tales' when reporting an incident.	**A just culture reporting system -** establish a reporting system that guarantees confidentiality of reporting individuals (a "just culture" reporting system) and include information on how to report breaches/occurrences via posters in staff rest areas.
	Induction training on reporting of security breaches - deliver training on the functioning of the "just culture" reporting system, its benefits and employees rights, responsibilities and duties in relation to occurrences as part every staff member's induction
	Rewards/Thank you - reward staff members who report security breaches and occurrences e.g. personal thank you from senior leaders, or recognition within the performance management system so that they know their report has been received and taken seriously.
INCIDENT RESPONSE	
DESIRED OUTCOME	TOOLS
All staff know how to respond and who to contact in the event of an incident.	**Wallet card** - issue to all employees a wallet-sized quick reference card containing details of who to contact for each type of security incident e.g. the number for reporting unusual or suspicious behaviour, reporting a lost company item etc. Cards could be made to fit into/to the back of airport/crew pass holders so to be always on hand.
	Regular table top exercises and practice drills – provide staff with the opportunity to think through the actions they may take during an incident and test their ability to respond to a situation. Lessons should be identified and recorded with changes in plans and procedures implemented where necessary.
INFORMATION SECURITY	
DESIRED OUTCOME	TOOLS
Sensitive information is stored, transmitted and disposed of securely and is shared only with those who need to know.	**Induction training** - deliver training on protecting and sharing information securely to all new employees with a test or other assessment to confirm understanding.
	Clearly documented information security policy and procedures – ensure this is readily accessible to staff who may want to refresh their understanding.
	Cyber Security - have robust cyber incident response plans in place. These plans should be tested and updated on a regular basis, with mechanisms in place to implement lessons learned

	from exercises and real life incidents.
	Reminder briefs - use briefings, handouts and posters in staff rest areas to remind staff of the importance of good information security, pointing out potential consequences of an information breach.
Lost/stolen items such as laptops, phones or papers are reported immediately.	**Wallet card/quick reference intranet page –** containing an easy to follow information on actions to take when company items have been lost or stolen.
MEASURES OF EFFECTIVENESS	
DESIRED OUTCOME	TOOLS
Improvements in security culture are being made.	**Breach records** - record the number of security incidents reported and allow an element of analysis to improve areas of weakness.
	Inspection results – record compliance rates with security policy e.g. number of staff correctly displaying their pass during inspections.
	Staff surveys/focus groups – carry out surveys to find out how staff feel about security and the culture.

— END —