Asia-Pacific
Economic Cooperation

Advancing Free Trade
for Asia-Pacific Prosperity

Building a Culture of Security and Countering the Insider Risk

BEST PRACTICES GUIDELINES

APEC Transportation Working Group

December 2022

Asia-Pacific
Economic Cooperation

Building a Culture of Security and Countering the Insider Risk

BEST PRACTICES GUIDELINES

APEC Transportation Working Group

December 2022

APEC Project: TPT 07 2020A

Produced by
U.S. Transportation Security Administration
6595 Springfield Center Drive, Springfield, VA 22150 USA
Tel: +1 571 227 1149
Email: Kalei.Hall@tsa.dhs.gov

For
Asia-Pacific Economic Cooperation (APEC) Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 68919 600 Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#222-TR-03.1

Table of Contents

Glossary

ACI	Airports Council International
APEC	Asia Pacific Economic Cooperation
AVSEC	Aviation Security
COVID-19	Coronavirus disease
CTWG	APEC Counter-Terrorism Working Group
GASeP	Global Aviation Security Plan
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
I-STEP	TSA Intermodal Training and Exercise Program
SeMS	Security Management Systems
SMS	Safety Management Systems
TAM	UNOCT Threat Assessment Models Programme
TPTWG	APEC Transportation Working Group
TSA	U.S. Transportation Security Administration
TWG	APEC Tourism Working Group
UNOCT	United Nations Office of Counter Terrorism

Executive Summary

Introduction and Approach

At the 2017 Asia Pacific Economic Cooperation (APEC) Transportation Ministerial Meeting, APEC reaffirmed its commitment to enhancing transportation security by:

- Improving Member Economies' capacity to mitigate vulnerabilities and counter terrorist threats;
- Engaging with other stakeholders within APEC (i.e., Counter-Terrorism Working Group (CTWG), Tourism Working Group (TWG)) and international organizations (i.e., International Civil Aviation Organization (ICAO));
- Encouraging participation in ICAO priorities, such as the development of Security Culture and human capability programs; and
- Minimizing security risks to transportation by encouraging economies to develop strong and informed security policies and to boost participation in security initiatives.

Similarly, ICAO emphasized that developing Security Culture and human capability are priority outcomes of the ICAO Global Aviation Security Plan (GASeP). To that end, ICAO designated 2021 as the "Year of Security Culture" (YOSC), further promoting and reinforcing effective Security Culture as a priority goal for international civil aviation. As a result, Security Culture became an important concept and imperative that economies, industry stakeholders, and aviation organizations championed throughout the COVID-19 pandemic to increase resiliency of the global aviation workforce and assist with recovery from the challenges presented to the international civil aviation system by the pandemic. Promoting Security Culture has ensured that security requirements are never compromised and that security awareness of all constituents within the aviation domain is of paramount importance.

In light of APEC's commitments and in-line with priorities of international aviation organizations, the United States proposed and received APEC approval for Project TPT 07 2020A – *Building a Culture of Security and Countering the Insider Risk*. The goal of this project was to assist APEC Member Economies in addressing and improving aviation and airport workers' engagement with and responsibility for security issues, as well as identifying and reporting behaviors and activities of concern to the appropriate authorities. The project highlighted that, by building a robust culture of security, these goals could be achieved without the need for major resource expenditures. The project assisted Member Economies in understanding the importance of Security Culture, how to design programs and policies that enhance security awareness and improve their organization's culture of security, particularly within the airport operating environment. The project also underscored the fact that an effective Security Culture and raising all constituents' security awareness can benefit the APEC region's aviation network, and ultimately the global transportation network, by establishing a safe, secure, and resilient system and community. The project also showed how the implementation of Security Culture has sustained benefits for every economy, which includes economies that are in the early stages of developing their aviation security (AVSEC) programs, as well as economies with more established AVSEC programs; regardless, it is particularly relevant for those operating with very limited AVSEC resources.

The objectives of the Project were three-fold:

1) Ensure participants understand the importance and concepts of Security Culture and how they relate to their domestic AVSEC regimes;
2) Increase participants' knowledge of the insider threat within the aviation domain and how to better leverage stakeholder buy-in to mitigate that threat within a resource-constrained environment; and
3) Build support for participants' strategies for implementing Security Culture concepts and best practices within their domestic operations, and employing risk analysis and mitigation principles.

This Best Practices Guidelines and the Project Summary, included at APEC Publication: APEC#222-TR-01.4, reflect the achievement of these objectives.

1 Introduction

The United States, as Project Organizer through the U.S. Transportation Security Administration (TSA), and on behalf of the project co-sponsors Canada, Chinese Taipei, New Zealand, and Singapore, is pleased to present this Best Practices Guidelines as a project deliverable to assist Member Economies in building an effective Security Culture and recalling best practices during the development and implementation process, in line with the 2020 Work Plan of the APEC Transportation Working Group (TPTWG).

This Best Practices Guidelines includes participant feedback, lessons learned, references and resources that were shared and agreed by the participants, speakers, and experts of the project.

1.1 Structure of the Document

This document is structured as follows:

- The **Executive Summary** introduces the project concept and its approach to building and implementing effective Security Culture in APEC.
- **Section 1** outlines the project's objectives and methodology, and describes the intended deliverables.
- **Section 2** explores Security Culture best practices from the Best Practices Guidelines, which is included in the Appendix.
- **The Appendix** complements the main document and outlines the Best Practices Guidelines.

1.2 Project Objectives

Security Culture is a set of common beliefs, values and practices that are inherent in an organization's daily operations. The benefits of Security Culture to an aviation organization are many, including the reduced risk of security incidents and breaches when employees work in more security-conscious ways. This has both direct and indirect impacts on an airport's commercial viability and consumer confidence – locally, regionally, and globally.

This project consisted of virtual workshop sessions, project evaluation instruments, such as questionnaires and mid-project and follow-up surveys, and the Outreach Campaign Briefer, culminating in a Best Practices Guidelines to enhance Member Economies' Security Culture policies and programs within the aviation domain. The workshops covered the benefits of conducting risk analyses, including identifying and defining key components of risk, and highlighting international practices and guidance on designing and implementing effective organizational security as a means of countering the unique risk posed by insiders within the aviation environment.

The objectives of this project were three-fold:

1. Ensure participants understand the importance and concepts of Security Culture and how they relate to their domestic AVSEC regimes.
2. Increase participants' knowledge of the insider threat within the aviation domain and how to better leverage stakeholder buy-in to mitigate that threat within a resource-constrained environment.
3. Build support for participants' strategies for implementing Security Culture concepts and best practices within their domestic operations, and employing risk analysis and mitigation principles.

1.3 Project Methodology

The target audience of this project were individuals in Executive or Managerial-level positions who are directly involved in the development and/or operationalization of AVSEC policies and programs within APEC Member Economies, both at the domestic (regulator) level and airport/industry (operator) level. It was imperative to have a good mix between regulator and operator level participants as the successful development and implementation of Security Culture requires a shared institutional mindset or ethos at both levels and throughout the aviation environment. Both need to work collaboratively to apply project principles and achieve project outcomes. Beneficiary profiles included Member Economy AVSEC officials, policy makers and regulators, as well as aviation industry stakeholders responsible for AVSEC.

Throughout the project, participants were required to complete and return pre- and post-workshop questionnaires by the end of the workshops, as well as participate in the mid-project and follow-up surveys. In these evaluation methods, each participant was encouraged to share their views and advice on the project's impact and efficiency as well as possible suggestions and policy implications for future APEC-related cooperation programs and activities.

All project activities, including workshops, were conducted in English.

1.4 Project Deliverables

As approved in the Project Proposal, the deliverables for the project were two-fold:

1. A Best Practices Guidelines (this document), which compiles the inputs from experts and participants collected during the workshops and project activities.
2. A Project Summary (refer to APEC Publication: APEC#222-TR-01.4), which outlines the details of the project.

2 Security Culture Best Practices

Throughout the project, participants were encouraged to share best practices to build a culture of security within their economy through the project evaluation instruments and during the workshop itself. The initial set of recommendations were captured from inputs from the Part 1 Workshop and included in the Outreach Campaign Briefer that was shared with participants in October 2021. The Briefer may be found in APEC Publication: APEC#222-TR-01.4. The Best Practices Guidelines, which may be found in the Appendix, expands on information already found in the Briefer and captures additional best practices and lessons learned over the course of the entire life of the project. The Guidelines provides key considerations participants noted throughout the project, as well as additional considerations where participants noted challenges in their own programs, namely where to start and how to develop or implement certain Security Culture Tools or principles. The Guidelines is by no means an exhaustive list of Security Culture best practices; however, it provides a true look at key principles explored in depth throughout the project and best practices, references and resources that participants and experts offered as crucial to building a culture of security and countering the insider risk.

Appendix – Best Practices Guidelines

REFERENCES and RESOURCES

This section provides valuable references and resources, many provided by the project participants and experts, which reinforce the best practices that can be found alongside. Additional Security Culture resources are included at the end of the Best Practices Guidelines.

Indonesia Directorate General of Civil Aviation Decree Number 55 Year 2021
https://www.dgca.gov.in/digigov-portal/

- DGCA of Indonesia issued Decree 55 Year 2021 as a reference for all stakeholders at the airport to implement aviation Security Culture

United Kingdom Embedding Security Behaviour Change
https://www.cpni.gov.uk/embedding-security-behaviour-change

- Provides a cohesive approach to creating a coordinated strategy for security behavior change, including off-the-shelf campaigns and guidance documents

Airports Council International (ACI) Airports Risk Assessment Handbook
https://store.aci.aero/product/airport-security-risk-assessment-handbook-first-edition-2020/

- Assists airports with guidelines for understanding threats, assessing associated risks, and allocating resources where they are most needed

OVERVIEW

From February 2021 to September 2022, the United States conducted Project TPT 07 2020A, entitled *Building a Culture of Security and Countering the Insider Risk*, under the auspices of the Asia Pacific Economic Cooperation (APEC). Project activities included a Part 1: Virtual Workshop held 16-17 June 2021, a mid-project survey, Part 2: Virtual Workshop held 8-12 March 2022, a follow-up survey, and pre- and post-workshop questionnaires. From the discussions and responses to the project evaluation instruments, key themes and best practices emerged and were captured in an Outreach Campaign Briefer, which was sent to participants midway through the project. This Best Practices Guidelines builds on those key themes and captures best practices from all project activities to assist economies with the development and implementation of their Security Culture.

Make a Plan

When thinking about how to build a culture of security, it may be daunting to decide where to start. As an organization explores what Security Culture Tools they might currently employ and those that they may want to implement or enhance, **having a plan is key** to choosing a goal, evaluating alternatives or activities to meet that goal, and deciding on the path to achieve that goal. To ensure the organization, as a whole, embodies and prioritizes a culture of security, **Security Culture principles should be included in the organization's Strategic Plan** with resources allocated, such as human resources and budgetary resources. Developing an Implementation Plan around the ideas and concepts included in the Strategic Plan involves outlining the tasks for completion, identifying personnel and resources needed, and documenting timelines. Having a plan provides concrete steps to achieving the principles committed to in the Strategic Plan, gives the implementers guidelines to stay on track, as well as a tangible document to share with leadership and stakeholders whose buy-in of activities are critical to success.

Understanding Threat in Risk-Informed Ways

To understand what aspects of Security Culture should be implemented or enhanced within the aviation ecosystem, organizations are encouraged to make risk-informed decisions by conducting risk assessments. **Risk assessments are an integral component to Security Culture and should be informed by current intelligence from government and open sources.** Through its Threat Assessment Model (TAM) Programme, the United Nations Office of Counter Terrorism (UNOCT) looks at the operational lifecycle of aviation security organizations as it manages risk to safeguard civil aviation against acts of unlawful interference and of counter-terrorism organizations as it identifies threats to prevent and counter terrorism. At points where the two organizations intersect, **mutually beneficial information sharing can occur when aviation security and counter-terrorism organizations have built a foundation of cooperation, communication, and trust towards the common goal of greater security awareness**. This relationship is also often solidified through legislation and reinforced through joint security exercises. This give and take between the 'need to manage risk' and the 'need to know' is key to enhancing information sharing between counter-terrorism organizations who may have

United Nations Office of Counter Terrorism
http://un.org/counterterrorism

- The UNOCT TAM Programme aims to consolidate multiple streams of expertise and assists economies to establish a common approach to threat assessments within the context of aviation security, build an interagency coordination model, and improve internal operational capacity to comply with international aviation security requirements

ICAO 40th Assembly SkyTalk: Aviation Security Risk Management
https://youtu.be/WDDIEUC1mlA

- Focuses on the ICAO aviation security risk assessment process, using methodologies found in ICAO Document 8973 and Document 10108, as well as its Risk Management Workshop

Capt Eddie Mayenschein, U.S. TSA, on Leadership and Building Relationships

- Encourage people to tell stories and listen to others as they tell their story
- It is okay to make a mistake; do not consider it a failure. Take the lessons learned and knowledge forward
- Be real and authentic. Be who you are in all circumstances
- Keep growing – you are always a work in progress. Be patient with yourself
- Energy is a valuable resource

Understanding Threat in Risk-Informed Ways (contd.)

intelligence that can be beneficial to incorporate into risk assessments conducted by aviation security organizations.

To assist with identifying and focusing on issues of critical risk, ask "What keeps me (or you) up at night?" Have conversations with aviation stakeholders about your concerns and ask them to share theirs. Often, concerns are collectively shared by other stakeholders throughout the aviation ecosystem, so identifying recurring concerns can help highlight and narrow the focus to the most critical risks. Additionally, when considering mitigation measures, **leverage the diverse thinking and perspectives available amongst aviation stakeholders to find innovative solutions**. Risk assessments should not be conducted in a vacuum, instead, consider inviting aviation stakeholders, such as airlines managers, aviation security authorities, and airport security coordinators to partake. **As risk-informed policy and program decisions are made, they should be documented along with the underlying rationale and shared with stakeholders**.

Risk assessments should be conducted regularly (e.g., annual, bi-annual, quarterly) to monitor and evaluate current operations, and they must be updated to account for any changes, such as: new threats (e.g., growing cyber threats from ransomware); newly identified vulnerabilities; and changes in the operating environment (e.g., major uptick in cargo operations due to COVID-19). As risk assessments change, perhaps due to the change in threat, these changes should be communicated to stakeholders in a timely manner. Stakeholders have an equal stake to ensuring the safety and security of the aviation ecosystem. Without their buy-in and belief that "security is everyone's responsibility," the system will not function as desired.

Building Stakeholder Relationships

A key to building strong stakeholder relationships is to **establish and foster trust and inclusion through consistent and meaningful engagement**. Relationships are a state of binding and building together, and as such, to build stakeholder relationships silos must be broken down and teams must be built with the highest level support, in which information sharing and coordination are robust and ongoing. Working without collaboration often misses opportunities to see the full picture, therefore organizations should invite and enable the active engagement and contributions of all stakeholders. Believing a single organization can understand all the security components and therefore continue to act solely of their own accord are barriers to building partnerships that advance security and innovation.

So how can one build a relationship with stakeholders to leverage buy-in on security issues? It is not easy and it does not happen overnight. It happens with one conversation at a time, so start by reaching out to people – both employees and stakeholders. **Be a visible presence** – walk the airport or office, invite stakeholders to meetings and attend them, exchange business cards, and engage in conversation. Planting the seeds now and watering them through quality engagement will establish

Capt Mayenschein (contd.)

- Things never happen exactly as they will – stay flexible
- You are already a role model. The question is what kind of role model are you?
- Your team will rely on you to invest in yourself
- The choices in life show us who we truly are, not our abilities
- There are three human freedoms: the power to choose, the power to respond, and the power to change
- To be a better leader, be a better human. To change your life, raise your standards
- It is what you are made of, not the circumstances that you are put in, that make the difference
- Leaders provide leadership in two ways – through the stories they tell (talk) and the kind of lives they lead (action)
- On the subject of mentoring, it is just as crucial to honor what is good and unique about your mentee as what you teach them
- Leadership is making others better just by being there. Influence is when you are not there and your absence is felt
- You do not have to be a person of influence to be influential
- Being there is how you change the culture. Being there provides the opportunity for influence but also to be influenced
- The circle around you is small, make everyone feel special
- Be humble – beautiful people do not ask for attention

Building Stakeholder Relationships (contd.)

the relationship in advance of a time where it is critically needed, such as during a critical security incident. **Trust must be the foundation of the relationship.** Ensuring that you pick up when the phone rings will demonstrate your commitment to the relationship and will encourage reciprocal responses when you are the one calling.

Leadership at Every Level

The ability to build and cultivate relationships is a critical component of being an effective leader. However, executive or senior leadership are not the only people responsible for cultivating relationships. As Capt Mayenschein stated, **"Everyone is a leader in their own way, leadership does not rest with a person nor does it require a title. It is a relationship among people."** Therefore, building employee and stakeholder relationships should be encouraged at all levels of the organization. The stronger the relationship between people and organizations, the greater the understanding that security is everyone's responsibility. Reaching out and having a conversation one day can lead to knowing who to call and rely on during a critical incident.

In regards to fostering a culture of security, the role of a leader is not to lead from the top-down but for all levels of the organization to exercise security leadership and demonstrate the importance of Security Culture. **Regardless of what level one is at within an organization, one can always embody the mindset of a leader and employ good leadership principles**. Best practices for fostering a leadership mindset, include: building relationships with those around you one conversation at a time; building trust within those relationships; and being open and available, including being open to listening to new ideas from anyone in the organization and stakeholders. Many organizations have developed "open door" policies for physical office spaces and virtually through emails and employee bulletin boards, as well as by empowering the workforce to offer their ideas for continuous improvement, giving them a stake in the security and well-being of the organization.

From the bottom up, to encourage leaders to recognize the importance of Security Culture activities and support its implementation, one must lead by example. Ensure you are promoting and participating in the culture of security that you want to see your organization adopt. Educate, invite and enlist your colleagues to also take part. This may grow a movement that cannot be ignored by the executive leadership. Along with the principle of show, and similar to building relationships with stakeholders, have conversations with executive leadership. An executive may be at the top of the organizational chart but if the workforce at every other level supports and calls for a greater commitment to a culture of security, then it cannot be easily ignored. As Capt Mayenschein said, "Do not stop until you are proud."

When a culture of security is established, it is essential for the workforce across the aviation ecosystem to embody effective Security Culture principles every day, including new employees from the first day of hire. To achieve this, Security Culture principles can be and are often

Capt Mayenschein (contd.)

- Leaders ask questions to diverge from their current thinking. Surround yourself with diverse perspectives
- Those who do not risk, cannot win. If you get a chance, take that chance
- Ask the people you work with, what can I do to make you successful?
- A professional does the things they love to do even on the days they do not feel like doing it
- Insecure people are loud but confident folks are quiet. Believe in yourself
- Bring your mind to work each day, but do not forget to also bring your heart

Chile Aviation Security Reporting System
https://servicios.dgac.gob.cl/avsecreportes/#/

- A voluntary and confidential system to report events that affect civil aviation security for use by passengers, crew members and ground personnel

Republic of Korea Aviation Security Voluntary Report System
https://www.kotsa.or.kr/eng/aviation/security.do?menuCode=05060000

- Aims to collect security risk information regarding any situation that endangers air safety

Leadership at Every Level (contd.)

incorporated into the on-boarding or new hire process, initial and recurrent training, and security awareness courses that may be conducted during the airport identification renewal process. In support of Security Culture, **aviation security executives should be a part of these presentations to share what their component of the organization does and to actively demonstrate top-level commitment to Security Culture principles.** Regular touchpoints (i.e., routine check-ins), emails, or newsletters to the workforce also reinforces that leadership is engaged in and actively promotes Security Culture principles and initiatives.

Benefits of Information Sharing

Meaningful relationships work together towards a common goal and shared purpose, such as the safety and security of the aviation ecosystem. Relationships are not a one-way street, there is a give and take. One benefit to building relationships with aviation stakeholders is the mutual sharing of information. While one organization may share the latest threat information at the local level, they may, in return, receive information on security occurrences at the airport level. No one organization can be everywhere at once so by sharing information, organizations may encourage sharing the responsibility for security and expanding the number of employees that operate with a security conscious mindset within the aviation environment. Information sharing can assist authorities with identifying vulnerabilities and the emergence of new threats and mitigating evolving ones, such as the Insider threat. **By sharing information and collaborating, organizations can be as dynamic and flexible in responding to threats and vulnerabilities – and security awareness is enhanced.**

Public Outreach and Awareness

Similar to the benefits of information sharing, public outreach and awareness can also encourage others, such as the travelling public, to travel with a security conscious mindset. Educating the public to stay vigilant, on what constitutes a suspicious activity, and how to report it further amplifies the number of eyes and ears that may notice a suspicious activity and make a report, increasing the opportunity for an in-real time response. In this regard, **having a clear reporting channel or mechanism available is essential.** A reporting mechanism can take many forms, such as a phone number to the airport security coordination center, a web-based reporting form or mobile application, or even the presence of law enforcement or other security personnel around the airport who can receive and respond to reports. The capability to allow for anonymous reporting should also be considered. **To encourage use of the reporting mechanism, it should be easily accessible and simple to use and recall when something happens.**

One way to encourage the public to report suspicious activities to the appropriate authorities is to **use strong visual and action-oriented components to convey the message**. This can include eye-catching posters, visual media, and announcements on the public address system at the airport, or information shared in advance of arrival at the airport (e.g., during the online check-in process). Within the aviation environment there are many distractions that can often cause sensory overload; therefore, security media, including messaging for suspicious activity reporting, should be bold and

U.S. *If you See Something, Say Something®* Campaign
https://www.dhs.gov/see-something-say-something

- A suspicious activity reporting campaign designed to educate the public on the threat and enhance awareness on the public's role in keeping communities safe

IATA "See It, Report It" Videos
https://www.youtube.com/playlist?list=PLM2XOQXtRLMfJrczSEG1syLwivOHW6YP9

- Short security awareness training videos, available in multiple languages

ICAO Security Culture Webinar
https://www.icao.tv/videos/the-icao-security-culture-webinar

- Highlights global security culture achievements in 2021 as part of ICAO's Year of Security Culture

Chile Civil Aviation Authority seminar: "Civil Aviation Security and Air Cargo"
https://www.dgac.gob.cl/con-exito-finaliza-primer-seminario-virtual-organizado-por-la-dgac-la-seguridad-de-la-aviacion-civil-security-y-la-carga-aerea/

- A seminar that brought together aviation stakeholders to address airport security, control and infrastructure, and considerations during the COVID-19 pandemic

Public Outreach and Awareness (contd.)

memorable enough to not be lost in the fray or compete for attention with other messages. Additionally, **it is important that the media should educate audiences on the evolving threat landscape.** If the public does not know what to look for and report on, particularly what threats are relevant to that airport or local area, then the quality of reports may be lower.

Public outreach and awareness campaigns are not just for the public, they also serve as reminders to the workforce and aviation stakeholders. **Partners should be encouraged to collect and share information through established reporting mechanisms.** This will simplify the process of reporting and allow ease of following up on reports if there is only one reporting mechanism and database to monitor, as opposed to one for airport workers and one for the public. Additionally, to encourage buy-in from aviation stakeholders for the program, **establish partnerships and use the organization's logo.** If the logo is well-recognized, it may spark positive "brand recognition" in the public. For example, if the airport authority has a logo or popular character associated with the organization, inclusion of these in the public awareness campaign media may draw additional attention to the messaging because it is endorsed by an established brand or relatable character.

Creating a contest or challenge around positive security reporting with the possibility of rewards or recognition can also be a strong incentive to encourage others to report suspicious activity. **When developing and implementing such programs, it is vital to understand what might motivate the intended audience or participants**. Often, organizations believe that rewards programs are costly; however, a simple poll of the intended participants might indicate that appropriate rewards could include simple actions as opposed to tangible goods. These could include recognition in front of peers during a ceremony or highlighting good security awareness events through newsletters and posters around the airport, which directly enhances participants' sense of belonging. Feeling a part of something is a strong intrinsic motivator and it promotes Security Culture buy-in. These types of outreach and awareness campaigns can be easily scaled and deployed across different modes of transportation, furthering the impact. Therefore, looking beyond the aviation environment is recommended to glean best practices and harmonize intermodal connections.

Lessons Learned from the Wider Transportation Network

Considering best practices and lessons learned from outside the aviation security realm may prove beneficial to organizations. Many of the security principles discussed, such as Security Culture and Security Management System (SeMS), started as and evolved from safety principles, such as Just Culture and Safety Management Systems (SMS). **Considering the merits of best practices and lessons learned from Safety Culture projects and campaigns that may be relatable to Security Culture may prove beneficial to your organization as it develops and implements its own projects and campaigns**. These insights might also provide an advanced starting point for your organization's projects, rather than starting from step one, or provide pitfalls to avoid.

U.S. TSA Intermodal Security Training and Exercise Program (I-STEP)
https://www.tsa.gov/for-industry/intermodal-security-training-and-exercise-program

- I-STEP activities provide the opportunity to review procedures that guide information sharing, implementation of physical protective measures, and operational coordination among industry employees, partners, and security stakeholders in the event of a security incident

ICAO Aviation Cybersecurity Strategy
https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

- Defines a common vision and global strategy on cybersecurity for the civil aviation sector through a series of principles, measures and actions contained in the seven pillar framework

U.S. TSA Cybersecurity Roadmap
https://www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf

- Identifies four cybersecurity priorities and six goals that will direct TSA's efforts to improve its protection of its internal Information Technology systems as well as the transportation systems of the United States

Lessons Learned from the Wider Transportation Network (contd.)

When considering the audience for your organization's security awareness campaigns, it may also be beneficial to consider intermodal transport operators who provide service to and from the airport. These may include mass transit, light rail, and bus operators, and taxi companies, which can provide additional eyes and ears actively vigilant for suspicious activities that should be reported. The transit companies may also be able to promote the campaign within its transport vehicles to act as another engagement touchpoint for the public, as well as lend additional confidence and credibility to the campaign itself. **Including intermodal transportation partners in other Security Culture activities, such as emergency exercise planning and tabletop exercises, not only expands the circle of engagement for Security Culture, but it also allows diverse perspectives and input for the activity outcomes**. Inclusion in such activities ensures that should a security incident occur, all aviation stakeholders and partners understand their roles and responsibilities. During and after conducting these exercises, it is vital to obtain feedback from the participants to take into consideration when adjusting any operational processes and procedures, as may be necessary to work for the specific scenario or in the current environment, if it has changed.

Including intermodal transportation partners that service the airport but do not necessarily work at the airport, encourages out-of-the-box thinking and more innovative alternative processes or procedures. By nature of not working for the airport or at the airport every day, these intermodal transportation partners may view the exercises and processes differently than those who do. These insights should be taken into consideration for any exercise or activity after actions or adjustments to processes and procedures in an effort to remain as agile as the threat.

Cybersecurity and Information Security

A bourgeoning threat in today's environment is cybersecurity, the consequences of which can range from theft of data to a potential act of unlawful interference. As with other aviation security concerns, **program development should start with a risk assessment and include the establishment of policies and procedures that support cybersecurity.** Connect and collaborate with local cybersecurity agencies to develop those policies and procedures. During the process, include relevant stakeholders and partners for support in managing the risks together. Once developed, share those policies and procedures widely. Cybersecurity is not limited to one area so a holistic and educational approach is key. **Conduct regular cybersecurity trainings and drills to ensure everyone is prepared to respond in the case of an incident.**

In the case of Information Security, best practices include the protection of sensitive aviation security information through the use of encrypted or password-protected documents, an intranet or other secured portal with limited access to those with a "need to know," and/or two-factor authentication, all layered with other mitigation measures, such as an Information Technology firewall system. Training on Information Security should be incorporated into the on-boarding process, induction and recurrent training. **Regular reminders on roles and responsibilities for the protection of Information Security and good cyber hygiene are helpful and may take the form of**

ICAO Security Culture Self-Assessment Tool
https://www.icao.int/Security/Security-Culture/Pages/State-self-assessment.aspx

- Provides a series of questions that can assist to assess if an effective Security Culture exists and identify possible areas of improvement

ACI Security Management System Workshop
https://aci.aero/programs-and-services/global-training/airport-security-training/security-management-system-workshop/

- Helps aviation operators understand the seven key components to SeMS and develop a comprehensive approach to security

Cybersecurity and Information Security (contd.)

notifications when accessing a secured system, as well as signed policy documents stating policies and procedures are understood by the employee.

Evaluating Processes and Programs

Understanding the insider threat and developing and implementing policies to mitigate that threat are layers to building an effective Security Culture. **Continuous evaluation of your organization's policies and programs is also necessary to determine whether they are achieving their intended outcomes and identify where improvements can be made.** As with all things, culture and the threat environment are not static. A periodic revaluation of Security Culture programs and policies is vital to ensuring that they are still effective for the current aviation environment, including for any new or emerging threat. Similarly, regularly conducting practice drills and exercises to test current procedures and responses is vital to ensuring everyone – the workforce, stakeholders, and partners – is trained and ready when an incident occurs. Conducting "hot washes" with participants, creating after-action reports, and acting on recommendations that may come out of these activities are essential to growing and enhancing one's culture of security.

To that end, **SeMS may assist with managing security in a cohesive, proactive, and risk-driven manner**. At its core, SeMS aims to embed security management principles into the everyday operations of the organization and its employees so that it is ingrained into the fabric of the organization itself. In this way, a SeMS program complements a culture of security through the everyday security actions of its people. With a focus on continuous improvement, SeMS can assist with incident management, management commitments, threat and risk management, resource allocation, performance monitoring and measurement, and quality management. Incorporating data analytic tools are one way to enhance SeMS programs and more quickly identify data trends to assist with performance analysis and identification of vulnerabilities, among other things.

ADDITIONAL SECURITY CULTURE RESOURCES

- Project TPT 07 2020A Materials: http://mddb.apec.org/Pages/search.aspx
- ICAO – Year of Security Culture: https://www.icao.int/Security/Security-Culture/Pages/YOSC-2021.aspx
- ICAO – Security Culture Toolkit and Resources: https://www.icao.int/Security/Security-Culture/Pages/ICAO-Resources.aspx
- ICAO – Security Culture Pamphlets and Other Campaigns: https://www.icao.int/Security/Security-Culture/Pages/Pamphlets-and-other-Campaigns.aspx
- ICAO – Cybersecurity Culture in Civil Aviation: https://www.icao.int/Security/Security-Culture/Documents/ICAO%20-%20Cybersecurity%20Culture%20in%20Civil%20Aviation_EN.pdf
- ICAO – Aviation Cybersecurity Strategy: https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

ADDITIONAL SECURITY CULTURE RESOURCES (contd.)

- Australia – A Guide to Developing and Implementing a Suspicious Activity Identification Program at Airports: https://www.icao.int/Security/Security-Culture/Documents/Australia%20-%20A%20guide%20to%20developing%20and%20implementing%20a%20Suspicious%20Activity%20Identification%20Program%20at%20airports.pdf
- Australia – Australian Cyber Security Centre: https://www.cyber.gov.au/
- Australia – Sydney Airport Security Awareness Guide: https://assets.ctfassets.net/v228i5y5k0x4/3NJHGSdSR3gM1giDE4a3iJ/141ae650cdefce75b37b557ed40be68d/Security_Awareness_Guide_V6.pdf
- Canada – National Cyber Security Strategy: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
- Indonesia – Year of Security Culture Presentation: https://www.icao.int/Security/Security-Culture/Presentations1/DGCA%20Indonesia%20%E2%80%93%20Security%20Culture%20Workshop.pdf
- Mexico – Publication on the Security of Civil Aviation: https://www.gob.mx/afac/acciones-y-programas/seguridad-de-la-aviacion-civil
- New Zealand – Aviation Security Awareness Video: https://www.youtube.com/watch?v=IHQUIVSuE7o
- New Zealand – Security Culture Newsletters and Resources: https://www.aviation.govt.nz/safety/security-culture/
- Singapore and United States – Information Sheet on Security Culture: https://www.icao.int/Security/Security-Culture/Documents/Singapore%20and%20U.S.%20-%20Information%20Sheet%20on%20Security%20Culture.pdf
- United States – "Building and Sustaining a Strong Security Culture Through Airport Community Security Awareness and Employee Recognition Programs: A Case Study from the United States" Article: https://www.icao.int/Security/Security-Culture/ICAO%20SC%20Resources/Building%20and%20Sustaining%20a%20Strong%20Security%20Culture.pdf
- United States – Transportation Security Administration Employee Recognition: https://www.tsa.gov/about/employee-stories
- United States – MyTSA Mobile Application: https://www.tsa.gov/mobile
- United States – Security Posters for Awareness Campaigns: https://www.cdse.edu/Training/Security-Posters/
- United States – National Insider Threat Task Force, Government Best Practices for Insider Threat: https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf
- ACI Asia-Pacific – Security Culture Explained Video: https://www.youtube.com/watch?v=STgTmVzzXyw
- ACI World – A Guide to Promoting and Assessing Security Culture for Airports: https://www.aci-asiapac.aero/media-centre/news/guide-to-promoting-and-assessing-security-culture-for-airports
- IATA – Improving Performance through Security Culture: https://www.icao.int/Security/Security-Culture/Articles/An%20Article%20by%20IATA.pdf
- IATA – Security Management System: https://www.iata.org/sems/

CONTACT US

Do you have additional best practices and/or resources to include? Please send your ideas and advice to Kalei.Hall@tsa.dhs.gov.