INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO)
ORGANIZACIÓN DE AVIACIÓN CIVIL INTERNACIONAL (OACI)

COMISIÓN LATINOAMERICANA DE AVIACIÓN CIVIL (CLAC)
LATIN AMERICAN CIVIL AVIATION COMMISSION (LACAC)

THIRD MEETING OF THE AVIATION SECURITY AND FACILITATION REGIONAL GROUP
(AVSEC/FAL/RG/3)
Lima, Peru, 17 to 21 June 2013

AVSEC/FAL/RG/3 — WP/28
14/06/13

Agenda Item 6: Aviation Security (AVSEC) and Facilitation (FAL)

FRAMEWORK FOR THE PROCUREMENT, TESTING AND DEPLOYMENT OF SECURITY EQUIPMENT

(Presented by United States)

SUMMARY

A consistent and standardized approach in the establishment of security equipment minimum specifications will assist States in the development of specifications for security equipment. A consistent and standardized approach to aviation security equipment standards setting and the establishment of process can also assist in ensuring the consistent screening of threat items. Factors of the standardized approach include security equipment procurement, testing and deployment.

Strategic Objectives	*This working paper is related to ICAO Strategic Objective B.*

1. Introduction

1.1 Recent aviation terrorist events have demonstrated how creative perpetrators of these planned attacks can be and have forced State authorities to take security measures to protect civil aviation against future potential terrorist attacks. Such measures include the development, procurement, and deployment of new, advanced technologies designed to detect threats of various complexities. While most countries have in the past made their own decisions in the deployment and implementation of such equipment, a consistent and standardized approach in the establishment of security equipment minimum specifications will assist States in the development of specifications for security equipment.

1.2 A standardized approach to aviation security equipment standards setting and the establishment of processes can go a long way in ensuring the consistent screening of threat items in an increasing number of countries. One could argue that this approach serves as a deterrent to would-be terrorists in trying to find gaps in the worldwide system of aviation security screening, when faced with overtly apparent consistency in both the equipment being used and the associated processes.

1.3 When making technology procurements, focus should be placed on the long-term goals while guiding through the acquisition life cycle. It is important to consider and communicate the proper combination of resources, requirements, and scheduling for successful acquisitions and sustainment. This requires developing documentation for projects that focus on the lifecycle of an acquisition.

2. Discussion

2.1 Procurement Framework

2.1.1 This framework is designed to be technology agnostic, meaning that the stated operational capability is more important than exactly how the system accomplishes the task. For each technology some details will be described to which each country can add to, depending on their own local risk assessment, operational constraints and other needs. A phased, systematic approach to technology and systems acquisition is a proven government and industry method for reducing acquisition risk and achieving more effective and efficient results from invested resources. The ultimate utility for the operational end-users is better constructed acquisitions, and better, more informed acquisition decisions. These, in turn, lead to a more predictable and effective delivery of capabilities. This emphasis should have an end result of performing quality analyses and gaining the knowledge necessary to support effective decision making.

2.1.1.1 **Planning:** Resources must be set aside for program management throughout the procurement process. Additionally, key resources (funding, testing support, etc.) should be designated and a general project plan should be developed to help guide the process forward. Validating that the project is on track and prepared to examine solutions is the goal of this stage.

2.1.1.2 **Solution Engineering:** In developing a system, a validation is needed to ensure the project will meet a desired capability. A consideration of other programs currently being perused should be considered as potential feasible alternatives to fill an identified gap. The main goal of this stage is to make sure that the project is within the areas of need and that redundancy of systems is minimized while all alternatives are considered.

2.1.1.3 **Market Research:** Emphasis should be placed on market research to match a technology solution to a project’s requirements. The roles of the design and development stages - transforming requirements into system design and converting system design into a solution - are then completed through the market research stage. Care should be exercised throughout this step to ensure that data collected and analyzed represents factual product capabilities, the vendor’s capacity to deliver, and relevant past performance.

2.1.1.4 **Concepts of Operations (CONOPS):** A CONOPS document is developed to outline how the technology will function and what capabilities the technology will have at the completion of the project life cycle. At a high level the CONOPS document should outline what impact the new technology will have on the day-to-day operations of the airport and should focus on an explanation of the technology’s capabilities.

2.1.1.5 **Requirements Definition:** Based on the initial results of market research, a baseline for a capable solution should be established. The basic requirements are developed based on the analysis of user requirements, documentation, and functional requirements of a solution. The setting of minimal specifications for security equipment requires an organization to follow a structured approach, which considers key elements that are integrated to achieve a specific security objective. The key elements for consideration in this approach are (1) threat identification; (2) detection capability and technology; and (3) operational requirements and considerations. Requirements drive technology solutions; therefore if

current technology solutions on the market are found to not meet a user's needs, a state can meet with the manufacturer on the need for further development of a technology to meet the user needs.

2.1.1.6 **Developmental Test and Evaluation (DT&E):** It is recommended that test and evaluation occur for equipment in a laboratory environment to explore and verify required functionality. These activities allow projects to assess available technologies, refine requirements, and verify technical conformance to specifications in a controlled environment prior to operational trials. During this stage of development, State scientists and engineers may collaborate with manufacturers offering relatively mature technology solutions to discover and implement design changes required prior to operational testing in order to meet a user's needs.

2.1.1.7 **Operational Test and Evaluation (OT&E):** Test and evaluation of qualified equipment in an operational test environment is conducted to independently validate whether candidate systems are operationally effective and suitable in an airport environment. OT&E focuses on the critical operational issues defined by the project sponsor and results of this testing should be considered by decision makers before a procurement decision is made. OT&E allows operators to confirm that the results of previous testing were valid and provides assurance that a system is ready be procured and deployed in the operational environment.

2.1.1.8 **Deployment:** At this stage a state is ready to acquire equipment and deploy capability to airports. The deployment of technology solutions may be complex due to technical interfaces and additional requirements of installing technology within airports. It may also involve deploying physically installed assets to a large geographic area with potentially many sites. An Integrator, separate from the technology manufacturer, may be used to perform this step if necessary.

2.1.1.9 **Operations and Maintenance (O&M):** This stage develops added focus due to the need for enhanced lifelong maintenance for detection technologies. Additional life cycle costs beyond the initial procurement should be accounted for within this stage, as they may ultimately exceed initial capital investments over time. These include the need for consumables and other compatible and interoperable systems within each capability area. Logistics and space requirements for consumables should be incorporated into the overall O&M plan.

2.2 Threat Identification

2.2.1 The identification of human and material threats against civil aviation, including those designed to seize and/or bring down an aircraft is the cornerstone of aviation security. State Security Authorities and Intelligence Services provide actionable intelligence on global terrorist organizations. These organizations are the ones that carefully analyse threat items that have been used in past incidents to make informed predictions regarding elements of capability and intent that may facilitate future attacks. This data, used properly, will assist government security authorities to best determine current and emerging threats.

2.2.2 Threats must be identified in order to inform security authorities who are charged with determining ways in which to counter them. Collecting these data from a variety of sources, both nationally and internationally, then collaborating within established State rules, requirements may be developed that provide adequate identification of such threats. In order to determine how to prevent the introduction of threat items or restricted articles in the sterile area or security restricted area, it is imperative that these items or articles first be identified with the threat that each may pose prioritized against the larger list.

2.2.3 In addition to threat identification, there should also be a thorough assessment of the type

of object and size required to cause major disruption to civil aviation such as the destruction of the aircraft or to use the aircraft as a weapon. Typically, complex research studies and analyses are conducted and reports will be generated to provide information that describes quantifiable and measurable characteristics of each threat item.

2.2.4 Perhaps, despite the effort to identify potential threats to civil aviation, other threats may emerge which will not have been part of the original assessment. Therefore, the requirement may have to be re-visited.

2.2.5 At a minimum, the following should be considered when identifying threat items or restricted articles.

- Guns and devices that discharge projectiles with sufficient velocity to cause damage to the aircraft or its occupants;
- Knives and sharp objects (metallic and non-metallic);
- Explosives;
- Improvised explosive device components;
- Stunning devices;
- Blunt instruments;
- Incendiaries; and
- Incapacitating sprays (such as Mace© or defensive pepper spray).

2.3 Detection Capability and Technology

2.3.1 Ultimate Detection Requirement

2.3.1.1 Once threat items have been identified, scientific analysis of the characteristics of the threats needs to be performed. These characteristics and properties will inform State authority officials to select and choose the appropriate technology to efficiently detect and mitigate the threat. The characteristics of the threat will also guide the State authority officials in their development of a minimum Detection Requirements document. This document is very sensitive and should not be made public, as Intelligence data may have been used to create it. In the U.S., these documents are guarded as State secrets and are classified. As previously stated, this document may also evolve over time.

2.3.1.2 The minimum detection requirement for a specific threat needs to take into account technology detection limitations, capabilities, and a scientific analysis/outlook for future potential improvement. International collaboration between States is an essential part of the process to establish minimum detection requirements for each deployed technology. For example, the minimum detection requirement for an X-ray device may be different from that of a trace detection system as these systems each “look” for threat signatures in very different ways.

2.3.1.3 Once the minimum detection requirement is established, an assessment of technology detection capability is the next step. This part consists of the selection of Key Performance Parameters (KPP) to conduct an evaluation of the required detection capabilities. The KPPs generally considered for security equipment are:

- Probability of Detection: the probability of detection (Pd) refers to the probability that detection system will detect a certain threat item under a given set of conditions;

- False alarm Rate (Pfa): there are 2 types of false alarms:
  - False Negative: a false negative occurs when a device fails to alarm in the presence of a threat item. This type of false alarm has an impact on security; and,
  - False Positive: a false positive occurs when a device generates an alarm even though no threat item is present. This mostly has an operational and measurable financial impact;
- Throughput: the ability to screen items or people quickly is very important. A system's "throughput" is a rate expressed in units such as persons per minute, bags per hour, etc.; and,
- Other key parameters, as outlined in State approved procurement documentation (example: automated detection, multi-view, image quality).

2.3.1.4 Ideally, Pd would be 100% and Pfa would be 0%. In practice this is never the case. If Pd is driven higher, Pfa tends to go up as well. A trade-off needs to be made, based on the maximum Pfa operationally feasible and minimum Pd required.

2.3.2 Technology Assessment

2.3.2.1 The technology assessment is carried out under ideal conditions in a laboratory environment following the intended concept of operations provided by the manufacturer. System performance is assessed based upon established requirements. Testing is conducted in a manner designed to evaluate as many variables as possible. This serves to provide repeatable test scenarios that fully address all stated requirements. All of the carefully scripted testing scenarios are catalogued and fairly applied to all representative manufacturer systems to be tested during the assessment, thus providing a comparison to benchmark data.

2.3.3 Performance Tools

2.3.3.1 The technology assessment provides the opportunity to develop test tools that will be used for future security equipment "proof of performance" and routine testing. The test tools, developed and referenced to the detection requirement during the laboratory assessment, can also be used to measure on-going field equipment performance.

2.3.4 Performance Standards

2.3.4.1 The information collected during the technology assessment will be used to support the creation of technical performance standards to be used to define the capabilities required of the current state of the art in security equipment. These performance standards will then become the reference for comparison and evaluation as technology may be further developed to meet a user's needs, and until they reach the ultimate detection requirement, as defined in 2.3.1.

2.3.5 Technology Improvement

2.3.5.1 Perhaps, despite the effort to identify potential threats to civil aviation the current state of the art technology may not be able to detect all those threats. The result may be that vulnerabilities remain.

2.3.5.2 A dynamic and progressive security technology program should ensure that the security system in place is capable of adapting to emerging threats as it considers improvements in technology and allows for regular review of the performance standards.

2.3.5.3 It is recommended that the detection requirement be structured to include progressive increments that will drive continuous technological improvement. This can be done by prioritization of threats, and other means.

2.4 Operational Requirements and Considerations

The operational requirements are usually part of the security equipment procurement cycle

2.4.1 Before operational deployment of a capability can be executed, the following must be considered.

- Size of items to be screened
- Space requirements (for systems, passenger queues, consumables storage, IT equipment, etc.)
- Size and mass of the equipment (e.g., floor loading, cooling requirements, etc.)
- Screening capacity (throughput, hourly screening capacity)
- Reliability, Maintainability, Availability (RMA)
- Integrity (possible sources of interference)
- Licensing (e.g. frequency bands used by the equipment, use of ionizing sources, etc.)
- Safety Requirements (for operators and passengers)
- Automation
- Operator interfaces / Human Factors
- Power requirements (e.g., simple plug in, or 3-phase hardwire, etc.)
- Data recording and information security
- Threat image projection capabilities
- Training requirements (both initial and recurring)
- Ease of use
- Environmental constraints (temperature, humidity, vibration, etc.)
- Networking, etc.

2.5 Deployment

2.5.1 Deployment Planning

2.5.1.1 This planning effort involves coordination among and participation of many critical functional disciplines and stakeholders to collect and assemble pertinent data. This is done to ensure that key aspects of fielding solutions are planned and implemented as designed. After the stakeholders are aligned and requirements are interpreted the next crucial planning effort is identifying and defining all tasks, task sequence, task duration, resource requirements, and deployment site selections. The deployment planning process provides capture and analyses of key stakeholder defined tasks, systems parametric and characteristic data, procurement schedules, equipment manufacturers production delivery schedules, coordination requirements, availability and readiness of key facilities, training needs, and approvals and certifications.

2.5.2 **Deployment Scheduling**

2.5.2.1 A key product of the deployment planning effort is called the Work Breakdown Schedule (WBS). This is the document that defines and organizes the total scope of the project. The schedule becomes a culmination of the WBS, along with the all defined tasks, task sequence, task duration, resource requirements, and deployment site selections. Also included are procurement data and technology manufacturer's production delivery schedules. Finally, this array of data is combined and aligned with key processes to form the deployment Integrated Master Schedule (IMS).

2.5.3 **Deployment Management and Execution**

2.5.3.1 Deployment Management and Execution (M&E) is major task area which overlaps into Planning as well as Transitioning due to the nature of this function. For example you may be in Program Execution for one technology while simultaneously managing Planning for a new technology, and also leading Transition for yet another technology. M&E involves implementation of plans and the performance of tasks/activities required to accomplish deployment objectives. The focus of M&E activities is the application of management methods, tools, processes, as well as key metrics to monitor program progress. Typical M&E practices include the use of management direction, weekly team meetings, monthly program reviews, resource allocation, quality assessments, and other program controls. The deployment program has numerous dependencies on externally managed processes that can potentially impact overall program performance.

2.5.4 **Deployment Systems Transition and Hand-Off to Operations**

2.5.4.1 Transition and Hand-off typically begins at T-0 (time minus zero) days (when equipment arrives on-site for installation). This is when the schedule "clock" for installation begins. This is the final preparation phase where local and airport application permits have been approved and subcontractors have completed pre-construction activities. The transition and hand-off to operations is in full-swing when the on-site team is in the process of transforming the site for system installation and security equipment is arriving and staged as required for the actual removal of old and installation of new security equipment. The equipment manufacturer support team brings the systems on-line and performs system site acceptance testing and certifies the system for operations. Airport operators receive training during the installation process. The systems are handed–off to operations under the control of trained operators and competent airport authorities.

3. **Suggested Action**

3.1 The Forum is invited to support the information contained in this Paper and encourage States to:

a) Develop security equipment procurement procedures that take into consideration the recommendations in the paper; and

b) Seek best practices from States that have followed similar procedures.

— END —