



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

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



**SECOND MEETING OF THE AVIATION SECURITY AND FACILITATION REGIONAL GROUP
(AVSEC/FAL/RG/2)**

Antigua and Barbuda, 16 to 18 May 2012

AVSEC/FAL/RG/2 — WP/08
02/05/12

**Agenda Item 4 Aviation Security (AVSEC)
4.2 Report on Communications / Information Exchange Project**

**REVIEW ON THE PROGRESS OF THE COMMUNICATIONS /
INFORMATION EXCHANGE PROJECT**

(Presented by the Communications / Information Exchange Project – Coordinated by Venezuela)

SUMMARY	
This Working Paper puts forward a report on the progress of the Communications / Information Exchange Project, on the aviation security information exchange and protection project assigned as part of the work for the Meeting of the Regional Group on Aviation Security and Facilitation (AVSEC/FAL/RG) held in Asunción, Paraguay, from May 25th to 27th, 2011.	
References:	
<ul style="list-style-type: none">• Programme and working projects related to the report of the First Meeting of the Regional Group on Aviation Security and Facilitation (NAM/CAR/SAM ICAO/LACAC)• Annex 17	
Strategic Objectives	<i>This working paper is related to ICAO Strategic Objective B.</i>

1. Introduction

1.1 During the last meeting of the Regional Group on Aviation Security and Facilitation (AVSEC/FAL/RG), for North America, the Caribbean and South America (NAM/CAR/SAM Regions) of the International Civil Aviation Organization (ICAO) and the Latin American Civil Aviation Commission (LACAC), held in Asunción city, Paraguay, from May 25th to 27th 2011, the ad-hoc group – integrated by the representatives of the United States of America, Panamá and Venezuela – was conformed in order to work on the Communications / Information Exchange Project, specifically on the Aviation Security Information Exchange and Protection Project; in accordance with Working Paper ND/01, approved during the before mentioned meeting and containing the AVSEC/FAL/RG proposed terms of reference, work programs and projects.

1.2 Established objects by the Aviation Security Information Exchange and Protection Project are:

- a) Maintenance of an updated database containing the regional officers responsible for the AVSEC branch.
- b) Development of an effective and efficient process to guarantee a reliable exchange of sensitive AVSEC information among the States, and
- c) Revision of the Guidelines for Management of Sensitive Aviation Security Information, presented by COCESNA (ACSA)

2. Progress on the update of the AVSEC Points-of-Contact (PoC) database

2.1 With the view to maintaining a unique updated database of the contact officers in each State to deal with issues related to AVSEC themes as to facilitate the exchange of information, with special interest to those cases where incidents may compromise people's lives and the aeronautical system continuity, a consultation process among the States began for the updating of the AVSEC Points of Contact List within the NAM, CAR and SAM regions.

2.2 The AVSEC/FAL/RG Secretariat issued by official letter No. LS 8/21.1 – SA018, of January 11th 2012, its considerations to the States of the NAM/CAR/SAM Regions in order to notify changes and confirm data related to their points of contact, intended to standardize the existing lists of the appointed officials in the ICAO AVSEC Points of Contact (PoC) Network as well as those appointed for the AVSEC/FAL/RG.

2.3 The States sent their answers to the before mentioned considerations. They resulted in the adjustments filed in **Appendix A** of this Working Paper.

3. Revision of the Guidelines for Management of Sensitive Aviation Security Information, presented by COCESNA (ACSA)

3.1 Based on the important contribution of the AVSEC Experts Group of Central America in cooperation with Regional Officers of TSA and ICAO, that resulted in the Guidelines for Management of Sensitive Aviation Security Information presented by COCESNA (ACSA) in Working Paper NE/17, during the last AVSEC/FAL/RG meeting held in Paraguay, a revision of such guidelines was performed and the adjustment recommendations that were arose are now presented in **Appendix B** of this Working Paper.

4. Progress on the design process for the exchange of AVSEC information

4.1 With a view to facilitate the exchange of sensitive AVSEC information among the States, investigations were performed in order to design a Draft Protocol for the exchange of AVSEC information. As a result of this investigation, it is evidenced that different initiatives have been internationally presented aimed at exchanging sensitive information (related to or different from the aviation security branch), and that such exchange do not compromise the security of the States engaged to the Agreement.

4.2 As an example of the before mentioned facts, there are initiatives as:

- a) the AVSEC information exchange system of MERCOSUR (SISME), conceived as a cooperation tool for the regional security branch, which offers the possibility to exchange information based on a communication platform jointly developed by the engaged States and the associated ones;
- b) the Memorandum of Cooperation between the Transportation Security Administration (TSA) of the US Department of Homeland Security (DHS) and the Latin American Civil Aviation Commission (LACAC);
- c) the enactment of a Draft Bilateral or Regional Agreement on Aviation Security presented by ICAO in Doc. 8973 (Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference), among others.

4.3 Fundamental aspects among the before mentioned examples are a legal structure that sets up parameters and conditions to handle information among the States that agree on the exchange. Therefore, bilateral and multilateral agreements represent the ideal framework to support the exchange of sensitive AVSEC information. Such agreements may grant the possibility to increase or annex to their content considerations related to the protocols or working methodologies that guarantee an adequate exchange of sensitive AVSEC information. In this respect, **Appendix C** of this Working Paper presents a Draft Agreement that considers the condition under which such exchange of information shall be performed.

5. Suggested Action

5.1 The meeting is invited to:

- a) urge the States to permanently notify the AVSEC/FAL/RG Secretariat about the changes that may arise during the appointment of the Points of Contact (PoC) related to the aviation security and facilitation field.
- b) provide the States with the Guidelines for Management of Sensitive Aviation Security Information, presented by COCESNA (ACSA), as well as with the suggestions proposed by this Project, in order to be considered as reference documentation for the standardization of criteria to properly safeguard information on aviation security, and
- c) subject the Draft Agreement on the functional protocol regarding an AVSEC information exchange system into the States' consideration and also take the actions that may be considered necessary.

APPENDIX B

**COMMENTARIES TO THE REVISION OF THE
GUIDELINES FOR MANAGEMENT OF SENSITIVE AVIATION SECURITY INFORMATION**

Commentaries of the AVSEC/FAL/RG Ad-Hoc group on the guidelines for management of sensitive aviation security information in order to complement the excellent work performed by the Central American AVSEC Group of Experts in cooperation with TSA and ICAO regional officers.

Page	Section	Original Version	Commentaries
5	Applicability	a. These procedures shall be applied to all airport operators, air operators, service providers and State institutions which have been provided with AVSEC information classified as secret, confidential and sensitive.	Each State may establish different levels and definitions for the classification of sensitive information. Therefore, we recommend mentioning at the end of the paragraph: <i>“... confidential and sensitive, or established under the classification defined by the State”</i>
5	Documents to be disclosed	Documents to be disclosed	We recommend to use the following expression: <i>“Documents to be under protection”</i>
5	Documents to be disclosed a 2	2. Relevant sections of national programs, rules and regulations, security test results, investigations and security circulars.	We recommend the following wording: <i>“National programs, rules and regulations, security test results, investigations, security circulars or the relevant sections related thereto.”</i>
5	Documents to be disclosed c. 1)	1. Security programs or relevant sections thereof to airline operators, service providers and State institutions.	We recommend that the following expression: <i>“State institutions or organizations”</i> be included in paragraph (a), considering that they depend on the State but not on the airlines.
6	Information classification	Information will be classified based on importance or type. The entity responsible for this classification will be the competent authority of each State.	Each State may establish different definitions for the classification of sensitive information. Therefore, we recommend to include a note that sets up: <i>“Note: In case of any divergences, definitions regarding information classification levels established by the State shall be mentioned”.</i>

Page	Section	Original Version	Commentaries
6	Document protection and marking a)	a. Printed documents, photocopies or electronic information (CD-ROMs, Diskettes, DVDs and USBs) must have an outer label with “secret, confidential or sensitive information” markings.	We recommend adding a phrase to establish that classification markings related to the sensibility of any information issued by a State may be accepted and used by another State in order to fulfill this requirement, according to the methodology used by each State for such classification.
6	Document protection and marking c)	c. Each paragraph will be marked according to the appropriate information classification level. The document or page will be marked based upon the highest classification of the paragraphs contained in it.	Paragraph marking based upon different classifications is a good practice. Nonetheless, it requires detailed guidance and wide training for the personnel in charge of document classification.
7	Sanctioning to custodians a) and b)	a. Persons responsible for safeguarding information who commit a violation/infraction will be subject to administrative and judicial sanctions according to the State law, if the information assigned under his/her responsibility has been used to commit or to allow acts of unlawful interference against civil aviation. b. Sanctions will be determined based on the results of investigations and the State’s national legislation and/or International Conventions.	Any kind of violation/infraction shall be reported to the competent authorities, even when incidents do not occur.
8	Custodial responsibilities b)	b. The responsibility of safeguarding information under custody shall be made clear and no information can be disclosed unless the established procedures have been followed and on the command of upper management.	We recommend that each State defines, within its internal procedures, the “superior level” that is authorized to order the disclosure of sensitive aviation security information, in order to identify and define responsibility levels towards such actions.

Page	Section	Original Version	Commentaries
8	<p>Custodial responsibilities</p> <p>e)</p>	<p>e. Information, which shall not be disseminated to the general public due to the vulnerability to the security system it represents, includes:</p> <ol style="list-style-type: none"> 1. Security program 2. Contingency plans 3. Security directives 4. Security inspections and their results 5. Investigation information 6. Threat information 7. Security training 8. Security tests 9. Security procedures 	<p>We recommend adding the following terms:</p> <p><i>“10. Detected vulnerabilities.</i> <i>11. Performance specifications required for security equipment, and</i> <i>12. Any other information which indicates specific measures, threats and risk level for an operation”.</i></p>
8	<p>Custodial responsibilities</p> <p>f)</p>	<p>f. In case of discovery any finding or incident related to this information, the person responsible for handling SSI shall notify upper management.</p>	<p>We recommend adding that the State will also communicate anomalies or incidents related to the information to the State providing sensitive information (if so).</p>
9	<p>Quality Control</p> <p>b)</p>	<p>b. Checklist shall include, at least, the following:</p> <ol style="list-style-type: none"> 2. Check classified information has not been left on desks, photocopiers, printers, fax machine or garbage collectors. 	<p>We recommend including the expression “Scanner”, in number 2, paragraph b).</p>

CENTRAL AMERICAN AVSEC GROUP OF EXPERTS

GUIDELINES FOR MANAGEMENT OF SENSITIVE AVIATION SECURITY INFORMATION

**FIRST ISSUE
04 JUNE 2010**

Table of Contents

Issue and Amendment Record..... 2
List of Effective Pages 3
Table of Contents 4
Objective 5
Applicability 5
Documents to Be Disclosed 5
Classification Levels..... 6
Information Classification..... 6
Document Protection and Marking..... 6
Control of Information within an Organization 6
Copy Control..... 7
Document Destruction 7
Sanctioning of Custodians 7
Custodial Responsibilities 8
Information to Other States 8
Quality control..... 9
Annex 1..... 10
Annex 2..... 11

CENTRAL AMERICAN AVSEC GROUP OF EXPERTS

OBJECTIVE

To adopt security measures for protecting aviation security documentation and to prevent it from being delivered to the wrong hands which may violate the AVSEC system.

APPLICABILITY

- a. These procedures will be applied to all airport operators, air operators, service providers, and State institutions which are provided with AVSEC information classified as secret, confidential and sensitive.
- b. States requesting information.

DOCUMENTS TO BE DISCLOSED

- a. State
 1. Annexes, manuals, relevant sections of these manuals, circulars and other documents.
 2. Relevant sections of National Programs, Rules and Regulations, Security Test Results, investigations and Security Circulars.
- b. Airport Operator
 1. Programs or relevant sections of the air operators' security programs, contingency plans, security circulars, meeting minutes.
 2. Rules and regulations.
- c. Air Operators
 1. Security programs or relevant sections of these security programs of air operators, service providers, and State institutions.
 2. Rules and regulations.
- d. Regional States
 1. Information provided by other States, programs, security circulars, intelligence reports of possible terrorist activities or criminal organisations that may affect civil aviation of each State.
 2. Third party information that may contribute to the aviation security system, maintaining the confidentiality of the persons that provided such information.
 3. Information provided during training to security personnel. A control system shall be used for the aforementioned statements.

CLASSIFICATION LEVELS

- a. Secret
- b. Confidential
- c. Sensitive

INFORMATION CLASSIFICATION

Information will be classified based on importance or type. The entity responsible for this classification will be the Competent Authority of each State.

- a. **Secret** All highly sensitive information considered a priority and that can only be known by a reduced number of persons.
- b. **Confidential** All medium level information related to aviation security and which may cause damage to the security system.
- c. **Sensitive.** All low level information that shall be disseminated to persons who require it for the performance of their tasks.

DOCUMENT PROTECTION AND MARKING

- a. Printed documents, photocopies or electronic information (CD-ROMs, Diskettes, DVDs and USBs) must have an outer label with "Secret, Confidential or Sensitive Information" markings.
- b. Information will be in headers, footers, and in a watermark, stating the classification level.
- c. Each paragraph will be marked according to the appropriate information classification level. The document or page will be marked based upon the highest classification of the paragraphs contained in it.
- d. Secret, confidential and sensitive information will be stored in a safe place determined by the competent authority.
Note: The competent authority should include, in an appendix to these guidelines, relevant detailed information about the custody of classified information.
- e. Photocopies, printouts and copies will implement the security measures established by the competent authority.
- f. Each user of an electronic device containing classified information shall have a unique access code.

CONTROL OF INFORMATION WITHIN AN ORGANIZATION

- a. All information will be property of the competent authority

b. A record of information received and provided will be maintained; this record shall satisfy, at least, the following requirements:

1. Name, signature and position of the person providing the information
2. Name, signature and position of the person receiving the information
3. Date and time
4. Amount of pages
5. Document classification

Note: Programs, regulations, security circulars, minutes, and training material will include a security code on each page as established in national documentation. A record of security codes shall be maintained.

COPY CONTROL

- a. In case, photocopies, printouts or electronic copies of any classified documents are required, a record of the amount of pages copied or printed, the date, time, name of the person who copied or printed the document, and the name person who requested them, will be maintained.
- b. The equipment used for copying and disseminating information will be for exclusive use and it will not be connected to any network.

DOCUMENT DESTRUCTION

- a. Documents classified as secret, confidential and sensitive will be destroyed when determined by the competent authority or according to national laws.
- b. Documents will be destroyed as determined by the competent authority (paper shredder, burning, etc) in order to prevent reading them.
- c. Destruction will be performed by at least two persons authorized by the competent authority.
- d. A document stating the type of material destroyed and the persons present during that activity shall be prepared.

SANCTIONING OF CUSTODIANS

- a. Persons responsible for safeguarding information who commit a violation/ infraction will be subject to administrative and judicial sanctions according to the State Law; this, if the information assigned under his/her responsibility has been used to commit or to allow acts of unlawful interference against civil aviation.
- b. Sanctions will be determined based on the results of investigations and the State's National Legislation and/or International Conventions.

CUSTODIAL RESPONSIBILITIES

- a. Persons responsible for handling information related to programs, rules, regulations, circulars, minutes or other shall be aware of the importance of this information in order to prevent claiming ignorance.
- b. The responsibility of safeguarding information under custody shall be made clear and no information can be disclosed unless the established procedures have been followed and on the command of upper management.
- c. No information that may put at risk the life of passengers, crew, ground personnel shall be disclosed.
- d. No civil aviation information that may put at risk the integrity of the States shall be disseminated to the general public.
- e. Information, which shall not be disseminated to the general public due to the vulnerability to the security system it represents, includes:
 1. Security program
 2. Contingency plans
 3. Security directives
 4. Security inspections and its results
 5. Investigation information
 6. Threat information
 7. Security training
 8. Security tests
 9. Security procedures
- f. In case of discovering any finding or incident related to this information, the person responsible for handling SSI shall notify upper management.

INFORMATION TO OTHER STATES

- a. Information can be shared with other States provided that they request it through a formal letter to the civil aviation competent authority.
- b. The information that can be share includes: programs, rules, regulations and data on threats to civil aviation.
- c. Information will be handled through the Department of Foreign Affairs unless, imminent danger exists; in that case and due to the lack of time, information will be provided by the civil aviation competent authority.
- d. The requesting State shall sign a confidentiality of information Memorandum of Understanding and notify the security measures to be applied to the information requested. In addition, the requesting State shall allow the State from which it is requesting information to verify it when necessary. (See Annex 1)

QUALITY CONTROL

- a. The person responsible for the custody and handling of classified information will conduct verification when beginning and finishing his/her tasks in order to corroborate information status. (include sample checklist, Annex 2)
- b. Checklist shall include, at least, the following:
 1. Check classified information pouches or containers are locked
 2. Check classified information has not been left on desks, photocopiers, printers, fax machines or garbage collectors.
 3. Check electronic devices used to copy and disseminate classified information are turned off.
 4. Check the office door is locked.
 5. Check other areas required by the competent authority.

CENTRAL AMERICAN AVSEC GROUP OF EXPERTS

ANNEX 1

MEMORANDUM OF UNDERSTANDING FOR THE PROTECTION OF SENSITIVE SECURITY INFORMATION BETWEEN (State or other providing entity) and (State or receiving entity)

This Memorandum of Understanding (MOU) details the procedures under which the (State or receiving entity) handles sensitive security information (SSI) in the material authorised by (State or providing entity) (herein after referred to as CAA).

The (State or receiving entity) understands that the SSI is to be protected from disclosure according to the legislation of (State or providing entity) based on the CAA's criteria that disclosing such information will be harmful to aviation security.

The (State or receiving entity) acknowledges it has received the SSI material and that the following procedures will rule the handling of such SSI material. The SSI material labelled as sensitive by the (State or providing entity) shall be:

- a. Protected from disclosure, unless a written authorization from the (State or providing entity) exists;
- b. Kept in the official facilities, unless an authorization from the (State or receiving entity) exists;
- c. Provided only to the organizations or persons considered suitable by the Director of the Civil Aviation Authority to access information and who have a "need to know" in order to perform or assist in an official authorized function;
- d. Accessible only to the authorized persons or organizations that have read and understood the SSI material handling procedures. These procedures shall not be disclose to a third party. Authorized persons or organizations shall comply with the terms of this memorandum of understanding;
- e. Handled only by authorized persons taking all precautionary measures to safeguard material and prevent unauthorized access by securing the SSI material in a container or in a locked door office when not being actively used. In addition, a list of persons provided access to the documents will be maintained;
- f. Copying is not allowed, unless it is necessary for operating purposes of the (State or receiving entity) and authorized by the Director of the Civil Aviation Authority of the (State or receiving entity), and

The (State or providing entity) approves the provision of the following SSI material to an authorized representative of the CAA of the (State or receiving entity):

- 1. National Aviation Security Programs
- 2. Contingency Plans
- 3. National Aviation Security Training Programme
- 3. Any other document related to the aforementioned material

By signing, the representative duly authorized by the Civil Aviation Authority (of the State or receiving entity) acknowledges receipt of the SSI material and the handling procedures of such material as stated above.

 Name: _____ Date _____
 Position:
 State

**ANNEX 2
Checklist**

CAA
representative: _____

Date: _____

Task	YES	NO	Remarks
Check classified information pouches or containers are locked.	<input type="checkbox"/>	<input type="checkbox"/>	
Check classified information has not been left on desks, photocopiers, printers, fax machines or garbage collectors.	<input type="checkbox"/>	<input type="checkbox"/>	
Check electronic devices used to copy and disseminate classified information are turned off.	<input type="checkbox"/>	<input type="checkbox"/>	
Check the office door is locked.	<input type="checkbox"/>	<input type="checkbox"/>	
Check other areas required by the competent authority.	<input type="checkbox"/>	<input type="checkbox"/>	

Remarks:

APPENDIX C / APÉNDICE C

**AGREEMENT ON THE FUNCTIONAL PROTOCOL FOR THE EXCHANGE SYSTEM
OF AVIATION SECURITY INFORMATION
BETWEEN
(NAME OF THE STATE) AND (NAME OF THE STATE)**

The (Name of the State's Institution) of (Name of the State) and (Name of the State's Institution) of (Name of the State).

CONSIDERING the (name of the bilateral / multilateral agreement), undersigned between (Name of the State) and (Name of the State) on (date).

TAKING INTO CONSIDERATION the necessity to defeat attacks against civil aviation security and to permanently progress towards the design of mechanisms for mutual cooperation and assistance on aviation security amongst the States within the region,

CONSIDERING the commitment of the States to strengthen aviation security information according to the provisions of Annex 17 – Security / Protection of civil aviation against acts of unlawful interference,

BEEING NECESSARY that the Aviation Security Information Exchange System allows an efficient and responsible access to information,

HAVE AGREED AS FOLLOWS:

Article 1

(Name of the State) and (Name of the State) agree to undersign the before mentioned Agreement on the Functional Protocol for the Exchange System of Aviation Security Information, annexed hereto and which shall be deemed to be integral part of the Agreement.

Article 2

The States commit themselves to adopt all necessary measures, according to the laws in force and to the material and human capacities available for each Party, in order to fulfill with the purposes of this Agreement.

Article 3

This protocol shall not restrict total or partial application of other instruments regarding the same field, already undersigned or those which may be signed between the Parties in the future, as

long as their provisions be more favorable to strengthen mutual cooperation on civil aviation security issues. The Parties may inform when the nature of such instruments is of their interest.

Article 4

This Protocol shall be indefinite in force. Nonetheless, either Party may at any time give written notice to the other Party of its decision to terminate this Protocol. Such notice shall be communicated (.....) month(s) in advance. In case of termination, both Parties shall adopt the necessary measures to protect the execution of aviation security operations from disruption.

Article 5

Any dispute arising between the Parties related to the interpretation or the application of this Protocol or due to failure of compliance with the provisions hereof shall be settle through consultations between the Parties.

This protocol shall come into force on the day of its signature by (Name of the State's representative) and by (Name of the State's representative).

Done in duplicate at....., the day of, all texts being equally authentic.

For (Name of the State)

For (Name of the State)

Annex
Functional protocol for the Exchange System of Civil Aviation
Security Information between (name of the State) and (name of the State)

General Considerations

Article 1

The Governments of (name of the State) and (name of the State), hereinafter referred to as the Parties, shall establish and maintain a common computer system called Exchange System for Civil Aviation Security Information, that may provide the appointed authorities, according to their functions, with efficient and opportune access to civil aviation security information, in order to protect civil aviation against acts of unlawful interference.

Purposes

Article 2

The purpose of this Protocol is to optimize security levels within the exchange processes of sensitive civil aviation security information between the States that agree hereto.

Cooperation

Article 3

For the purposes of this Protocol, cooperation shall include the exchange of sensitive security information, analysis and appreciations thereto, performance of coordinated operational activities, simultaneous and/or complementary and design of mechanisms to strengthen the civil aviation security field.

Cooperation may include other ways that the Parties agree according to their needs.

Resources

Article 4

Necessary resources for the implementation of this Protocol and for the achievement of its purposes shall be mutual responsibility between the Parties. Nonetheless, the Parties may agree, when necessary, other ways to bear the costs.

Structure

Article 5

The Exchange System for Civil Aviation Security Information shall implement a consultation system integrated by a national node, which shall be represented by the official or group of officials responsible for the collection of pertaining communication within each State and for any kind of interface between the States and the exchange system of civil aviation security information.

Article 6

The national node shall be managed by the competent authority on aviation security within each State. Such authority shall be responsible for the proper operation of the before mentioned

national node and shall adopt the appropriate measures to guarantee the compliance with this Protocol.

Article 7

The Parties, through their respective national representatives, shall cooperate to prevent and/or take effective actions towards acts against civil aviation security, provided that such actions are not reserved by law to other authorities and as long as such requested actions do not infringe procedural or substantive law.

Article 8

Nothing in article 7 shall be deemed to be opposed to direct cooperation between the competent authorities in the civil aviation security field, within their respective jurisdictions and faculties, if operative emergencies may arise. The Parties shall immediately notify each other of such emergencies.

Use of Information

Article 9

The information contained in the Exchange System for Civil Aviation Security Information shall not be publicly used or known.

Article 10

Information shall be exchanged according to the legislation in force of each Parties and based on the principles of reciprocity and celerity.

Article 11

The Parties shall take all proper measures to guarantee that handling and destiny of the information do not deviate from its original purposes or affect people's rights.

Article 12

The Parties agree to take special measures to prevent the knowledge and use of information by persons other than the recipient, or third parties not expressly authorized here at to access to such information.

The above mentioned security measures shall be referred to the protection and procedure for sending and reception.

Article 13

Each Party shall establish sanctioning measures for those who, intentionally or with negligence, allow unauthorized parties to know data contained in the Exchange System for Civil Aviation Security Information.

Exchange of Information

Article 14

The requests for cooperation and information exchange set forth in this Protocol, unless the provision in Article 16 should be handled directly between the competent national authorities in the aviation security field, through the Exchange System for Civil Aviation Security Information. The word “urgent” shall be printed on the request filed by the National Section of each Party in order to be processed.

Article 15

The Parties shall set up validation procedures for consultations and answers produced by the Exchange System for Civil Aviation Security Information in order to guarantee the authenticity of the national node as well as the information itself.

Article 16

The Parties shall establish mechanisms to ensure the expedite flow of structured information. In case such information is not available or not fully pertinent to the requesting Party, the Parties shall mail each other, unless legal impediment, to exchange information in the shortest time possible.

The word “confidential” shall be visually printed, when requesting or replaying pertinent information.

Article 17

The information requested under the provision of this Protocol shall be provided by the Parties according to their respective laws in force. Same conditions shall apply between both Parties.

Article 18

Without prejudice of the above, either Party may postpone the process of a request or subject it to conditions, if it interferes with an ongoing investigation within the scope of its jurisdiction.

Article 19

- At demand of the requesting Party, either Party shall maintain the confidential character of the consultations and answers. If it cannot be processed without infringement of confidentiality, the requested Party shall notify about such situation to the other Party, who shall decide whether the application remains in effect.

- In the same manner, the requested Party may ask for the confidentiality of the provided information. In such case, the requesting Party shall respect the conditions established by the requested Party. If the requesting Party cannot accept them, it shall notify the latter, which shall decide on the provision of the cooperation.

Article 20

The Parties shall inform each other, as soon as possible, on the compliance status of the application.

Article 21

When necessary, the application must be filed in the language of the requesting Party and a translation in the language of the requested Party shall be enclosed. The resulting reports shall be only written in the language of the requested Party.

— END —