International Civil Aviation Organization
South American Regional Office - Regional Project RLA/03/901
REDDIG Management System and Satellite Segment Administration
Twentieth Meeting of the Coordination Committee (RCC/20)
Lima, Peru, 21 to 23 March 2017

Agenda Item 3: **Report of the activities carried out to date since the last Coordination Committee meeting**

THE DSNA APPROACH REGARDING SECURITY

(Information Paper presented by FRENCH GUIANA)

SUMMARY

As States use information passing through REDDIG, we can consider REDDIG as a telecom provider.
This paper provides some rules used by the DSNA, the French ANSP, with the mainland telecom providers.

1. Introduction

1.1. Information technologies are a vital part of air navigation services and civil aviation in general. ATM systems need continuous flows of information and these data require confidentiality, integrity and availability performances.

1.2. But we are exposed to an increasing and continuous threat of attacks. Those attacks could be conducted by individuals, corporations or States and even ANSP internal staff may represent a threat intentionally or unintentionally.

1.3. States and organizations have to face those threats and take measures to contend with threats.

2. The French Air Navigation Cyber Policy (Information systems security policy)

2.1. The French Civil Aviation Authority (DGAC) is an administration and, like other French administrations, has to implement cyber security in line with the ANSSI (Information systems security national agency) recommendations.

2.2. The DSNA, the French ANSP, use this cyber policy to give the guidelines / good practices, secured architectures, methods, tools, and procedures to contend with the exploitation of the vulnerabilities.

2.3. This cyber policy needs to be re-evaluated regularly as threats evolve over time.

3. The DSNA approach

3.1. For each new change in the information system, the DSNA uses a process to assess the cyber risk.

3.2. We use the EBIOS (expression of needs and identification of security objectives) methodology which can identify the risks and a security policy adapted to our needs.

3.3. In case of changes including mainland telecom provider, we use this assessment to define measures and requirements that telecom providers have to implement.

3.4. These measures and requirements include the access management, the physical protection, the network segmentation, the configuration management, the mastering of the staff operating, audits, network cyber monitoring, etc.

3.5. At the same time, we also define security objectives to be applied by each center connected to the network.

3.6. This entails access management, security infrastructure and audit to validate the implementation.

4. Action by the meeting

4.1. The meeting is invited to note the information provided in this paper.

4.2. The meeting is invited to consider the need for the definition of a Reddig2 cyber policy, and for its application as soon as possible.

- END-