International Civil Aviation Organization SAT/22/WP/14
Twenty second Meeting on the improvement of Air Traffic Services over the South Atlantic (SAT/22) 15/05/17
Paris, France, (7-9 June 2017)

Agenda Item 3: **Communications, navigation and surveillance (CNS) (By CNS Working Group)**

NETWORKS CYBER SECURITY

(Presented by DSNA - French Guiana)

SUMMARY	
Networks between ANSP are vital for the safety of Air Traffic Services. This paper proposes to assess the security of each network.	
References :	RCC/19 Preliminary report RCC/20 Preliminary report

1. Introduction

1.1. Information technologies are central to air navigation services and civil aviation in general. ATM systems require continuous flows of information and these data require different levels of confidentiality, integrity and availability performances.

1.2. All air traffic actors, especially ANSP, are a target for cyber-attacks today. The threats are real and can take several forms depending on the means of the hackers.

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

1.4. Organizations have to identify their critical information systems and implement appropriate security measures in complement to existing cyber security objectives.

2. Discussion

The French Air Navigation security Policy (PSSI: Information systems security policy)

2.1. The French Civil Aviation Authority (DGAC) is an administration which, like other French administrations, implements cyber security in compliance with the European NIS (Network and Information Security) directive. The ANSSI (French National cyber security Agency created in 2009) defined and published the CIIP Law (Critical Information Infrastructure Protection). This law is compliant with the NIS directive. The law aims at reinforcing the cyber security of critical operators and allows ANSSI to further support them in the event of a cyber-attack against their critical information systems.

2.2. The DSNA, the French ANSP, has published its own security policy. Relying on the ANSSI recommendations, it defines guidelines / good practices, secured architectures, methods, tools, and procedures to contend with the exploitation of the vulnerabilities. The DSNA manages its own security risks through a global process by taking into account threats, vulnerabilities, and different criteria.

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

Internal cyber activity within Cayenne Regional Control Center

2.4. Before implementing the AMHS, which will replace AFTN, we will need to install a new aeronautical messaging system and we will have to look into cyber risks.

2.5. This equipment will be connected to the other ANSPs via VSAT networks (REDDIG II or Afisnet), the airport operators and the Air Force.

2.6. Potential threats could come from each of those actors and we need to install a new security system to ensure the cyber requirements on our equipment.

REDDIG II security

2.7. Last year, an ad hoc group was formed with members from Argentina, Brazil, Colombia, French Guiana, Paraguay, Peru and the REDDIG Administration. They analyzed the security of REDDIG II and classified the threats into two levels, internal and external.

2.8. Internal threats could come from the operator of the terrestrial network, VPN access via Internet, or human factors.

2.9. External threats could be caused mainly by users and their equipment connected to the REDDIG II. Radiofrequency interferences were also considered as a “threat” to network operation and security.

2.10. During the last RCC, the analysis was presented and the ad hoc group will prepare an action plan to mitigate the threats.

2.11. **Proposition**

2.12. The meeting is invited to assess the cyber issues on all systems and networks if the analysis has not yet been made.

2.13. The meeting is invited to consider the need for a cyber policy over SAT region, which would assess all issues: the definition of common threats scenarios, training, performances, security studies, audits and controls.

2.14. The meeting is invited to consider the work already achieved with REDDIG II, and the need for a systematic process of cyber risk evaluation on all new systems.

3. Suggested actions

3.1. The meeting is invited to consider propositions provided in this paper.

-END-