INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

REPORT OF

THE SECOND MEETING OF SECURITY SUB-WORKING GROUP OF ATN IMPLEMENTATION COORDINATION GROUP OF APANPIRG (ATNICG S-SWG/2)

Bangkok, Thailand
25 September 2008

The views expressed in this Report should be taken as those of ATNICG S-SWG/2 Meeting and not of the Organization. This report will be submitted to the Fourth Meeting of ATNICG for further action.

1. HISTORY OF THE MEETING

1.1 The Second Meeting of Security Sub-Working Group of ATN Implementation Coordination Group of APANPIRG was held at Pathumwan Princess Hotel, Bangkok on 25 September 2008.

1.2 Mr. Vidyut Patel, Security Engineering Group Manager, Air Traffic Organization, FAA, referring to the First Meeting of the Security Sub-Working Group highlighted that the primary task of the meeting would be to review the proposed Security Checklist.

2. ATTENDANCE

2.1 The Meeting was attended by 25 participants from 8 States (Hong Kong China, Fiji, India, Malaysia, New Zealand, Singapore, Thailand and USA). The list of participants is provided in **Attachment 1**.

3. OFFICERS AND SECRETARIAT

3.1 Mr. Vidyut Patel, Co-chairman for the ATNICG Working Group chaired the meeting.

3.2 Mr. Li Peng, Regional Officer CNS acted as Secretary for the meeting who was assisted by Dr. Sujan Saraswati, Regional Officer CNS of ICAO Asia and Pacific Regional Office.

4. ORGANIZATION, WORKING ARRANGEMENTS AND LANGUAGE

4.1 The ATNICG S-SWG/2 met as a single body. The working language for the meeting was English inclusive of all documentation and this Report. The list of Working Papers and Information Papers are placed in **Attachment 2**.

5. AGENDA OF MEETING

5.1 Following agenda was adopted by the meeting:

Agenda Item 1: Adoption of Agenda

Agenda Item 2: Review the First Security Sub-Working Group Meeting Report.

Agenda Item 3: Review follow-up actions to action items from the First Security Sub-Group Meeting.

Agenda Item 4: Review the Proposed Security Checklist

Agenda Item 5: Review System-Wide Contingency Document

Agenda Item 6: Review the System-Wide Incident Reporting Document

Agenda Item 7: Any other security related issues

Agenda Item 1: Adoption of Agenda

1.1 The meeting adopted the provisional agenda (WP201) without any change.

Agenda Item 2: Review the First Security Sub-Working Group Meeting Report

2.1 Mr. Vidyut Patel presented the First Security Sub-Working Group Meeting Report. There were no exceptions noted with the report.

2.2 It was noted by the Security Sub-Working Group that during the ATNICG WG/4 review of the outcome of CNS/MET SG/12 and APANPIRG/19, there was an issue raised concerning the Asia/Pac System Security Policy. The CNS/MET Sub-group, while reviewing and recommending for adoption of the Draft Conclusion "Asia/Pacific Aeronautical Telecommunication Network System Security Policy" was of the opinion that Security being a global issue should be guided by a global policy to maintain uniformity all over the world. The meeting was also of the view that the issue should be addressed by the Aeronautical Communication Panel (ACP). APANPIRG also took note of the opinion expressed at CNS/MET SG/12. In response to the observation made in CNS/MET SG/12, USA informed the ATNICG WG/3 meeting that at present, they were not aware of any Information Security Policy which includes Security Certification and Accreditation in the agenda of the ACP or any of its working groups. The meeting was also informed that Security, to an extent was being discussed in ACP was only in the context of technical provisions and guidance for securing Ground/Ground and Air/Ground communication. The ATNICG WG/4 meeting came to a conclusion that the scope of the document needs to be determined relative to AMHS support only and relative to ACP Policy. This issue was referred to the subsequent Security Sub-working group meeting for further discussion.

Action Item 1: Determine the scope of the Asia/Pac System Security Policy relative to AMHS support only and relative to ACP Policy.

Agenda Item 3: Review follow-up actions to action items from the First Security Sub-Group Meeting

3.1 Mr. Vidyut Patel reported that the primary focus since the first meeting was to convert the controls identified at that meeting into a Checklist format.

3.2 The other actions from the first meeting will be addressed at the ATNICG WG/5 meeting. These actions include expanding the Security Technical Guidance Document to cover Management and Technical Controls to correspond to the Checklist; to further develop the Contingency and Incident Response documents, and develop a strategy for a Regional ATN Monitoring Capability/Support that would encompass security incident response.

Agenda Item 4: Review the Proposed Security Checklist

4.1 Mr. Vidyut Patel presented the Proposed Security Checklist document. He reported that in order to ensure that security measures are implemented throughout the Asia/Pac ATN, a comprehensive checklist is needed. The ATNICG Security Sub-Group decided at the first sub-group meeting in April 2008 to base the checklist on the list of security controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (SP800-53).

4.2 Mr. Patel explained that the aim of the Security Checklist document is to identify security controls in checklist format, that is, is to describe each security control in a fashion suitable for an organization to verify that a set of controls sufficient for their operating environment has been implemented in accordance with the Asia/Pacific System Security Policy. This checklist may be used as the basis of an organization's *verification* that their system is implemented with appropriate security measures. With this checklist filled in the organization's Designated Approving Authority can provide *authorization* that the system may be placed into operation.

4.3 Malaysia asked if the checklist was specific to AMHS. It was reported that in its current form the checklist is generic and could be used be used for other systems as well. However, the selection of controls from SP 800-53 at the First Security Sub-Group meeting was based on applicability to AMHS.

4.4 Fiji asked if security was being moved to the Conformance Test work activity. It was reported that only the interoperability work is being moved there. The Security Policy was previously called the System Integrity Policy because Interoperability was included in the policy. Interoperability was deleted from the Security Policy.

4.5 While reviewing the Incident Response Checklist items India asked if there was a definition of a security incident. NIST SP 800-61, "Computer Security Incident Handling Guide" defines a security incident and gives typical examples. An incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Example incidents include Denial of Service, Malicious Code, Unauthorized Access, and Inappropriate Usage. The Security Sub-Group will be developing an Asia/Pacific Incident Response document using SP 800-61 as one of the reference documents.

4.6 Malaysia asked if the Security Checklist is part of ICAO Safety Checklist and would be used in ICAO audits. This checklist would not be used for formal ICAO audits since they must be based on provisions in the Annexes.

4.7 India asked if there are specific products to meet the checklist. The Security Guidance document will specify techniques to implement technical controls but not specific products. This led to a broader discussion on the use of the checklist. The meeting noted that if one node in the ATN is compromised, the whole network is at risk. Therefore the checklist should be applied on a global basis.

4.8 The ICAO Secretary asked about security issues associated with the Autoconfiguration capabilities of IPv6. The meeting was informed that in the Security Guidance section of Part III of Doc 9896 there was a specific section on "General Guidance for Implementation of Security". This section points to key IETF Informational RFCs that address IPv6 security issues including issues with Autoconfiguration.

4.9 The meeting then discussed the next steps and how to best adopt the Security Checklist document. It was agreed that the checklist items would be further refined at the upcoming ATNICG WG/5 meeting with the objective to reduce the 42 page document. It was not yet decided on how to adopt the document. One suggestion was to identify it as a "best practices" document. It was decided to continue to work on the document before deciding how to adopt it. After the ATNICG WG/5 meeting the document will be compared with similar material prepared by the AFSG. Mr. Patel will then coordinate with AFSG at their March meeting. This will then be reported on at ATNICG/4 in Singapore where it can be decided how adopt the document by APANPIRG.

Action Item 2: Coordinate Asia/Pacific Security Checklist with AFSG document and develop an approach to adopt the Checklist.

Agenda Item 5: Review System-Wide Contingency Document

5.1 Mr. Patel reported that work on the System-Wide Contingency Document would progress with a proposed outline to be presented at ATNICG WG/5.

Agenda Item 6: Review System-Wide Incident Response Document

6.1 Mr. Patel reported that work on the System-Wide Incident Response Document would progress with a proposed outline to be presented at ATNICG WG/5.

Agenda Item 7: Any Other Security Related Issues

7.1 No additional issues were identified.

6. ACTION ITEM SUMMARY

6.1 In addition to progressing the work assigned to the Security Sub-Working Group the following specific action item was agreed to by the meeting.

Action Item 1: Determine the scope of the Asia/Pac System Security Policy relative to AMHS support only and relative to ACP Policy.

Action Item 2: Coordinate the Asia/Pacific Security Checklist with the AFSG document and develop an approach to adopt the Checklist.

– – – – – – – – – – – –