RTCA Paper No. 247-21/SC224-165
September 20, 2021

Summary of the Seventy-Ninth Meeting

Special Committee 224 Plenary

Airport Security Access Control Systems

The seventy-ninth meeting of SC–224 was held virtually on September 2, 2021.

Attendees included:

Christer Wilkinson (Co-Chair)	AECOM System Solutions
Jose Chavez (Acting Co-Chair)	TSA
Art Kosatka (Secretary)	TranSecure Inc.
Djhanice "DJ" Neric (Government Authorized Rep)	FAA
Karan Hofmann	RTCA, Inc.
Jonathan Branker	FAA
Suzanne Guzik	CTI Consulting
Nancy Ford	Security 101
Walter Hamilton	IDTP
Kristina Dores	TranSecure Inc.
Lars Suneborn	IDTP
James McGuire	TransSecure Inc.
David McGhee	R&B
Ann Barry	R&B

Regrets: None

SC-224 – Meeting No. 79
(September 2, 2021 Meeting)

1. Welcome and Administrative Remarks:

Ms. Hofmann opened the meeting with the reading of the reminders for Anti-Trust Requirement, RTCA Proprietary Policy and Membership Policy and relevant exemptions. Dr. Wilkinson presented the agenda for today's meeting.

2. Approval of Previous Meeting Summary:

The Summary for the Plenary #78 (July 19, 2021) meeting was approved as published.

3. TSA Report:

Mr. Chavez, TSA representative, reported no currently relevant agency status or activity to report. He repeated his previous report that the Agency is working on cyber security guidance for national issuance; the TSA has issued 2 related Security Directives, including one for pipelines, but the issue remains under development to aim for national aviation industry guidance, not just SDs. Target is estimated for perhaps 6 months, to be in line with national cyber incident reporting guidance. There is also UAS guidance in the works.

4. Safe Skies Reports:

Ms. Guzik reported that Safe Skies Report (34) - Optimization of Video Systems– 1st draft is due Oct/Nov time frame in order to finalize in the Spring.   This not an update, but a new document.

Dr. Wilkinson reported that one new Safe Skies document - Access Control System Transitions (30) has recently been issued, and another on Security operations centers layout (43) is in preparation.

Mr. Kosatka noted they are likely to be somewhat redundant with and/or impact some sections of the TSA Guidelines document, including the SOC section, noting that in some airports the SOC and other functions share the same room.

Ms. Barry noted Safe Skies is also beginning an identity management project (48) which will likely have some bearing on DO-230L; she will contact Mr. Zoufal for coordination of his section.

5. Document Distribution

Ms. Hofmann reported that ACI (through Mr. Chris Bidwell) has received the newest version of our document (DO-230K). He acknowledged distribution of the previous version (DO-230J) to 69 members that had requested it.

6. DO-230L Preparatory Measures

Ms. Guzik has taken the current DO-230K and broken out each section to provide to section leads for edits and corrections for DO-230L preparation. Individuals are directed to keep all changes within those drafts to RETAIN common formatting throughout.

7. Section Reports

Mr. Suneborn reported that the access control industry's front end is currently very stable; the back end is where things are changing, the new Technology Alliance project is just beginning, with NIST starting on implementation policies for the Federal sector.

In the federal requirement sector, the Next Generation Access Control, NGAC, is expanding the FIPS 201/ FICAM (Federal Identity Access Management) Next Generation Access Control is a fundamental reworking of traditional access controls to meet the needs of the modern, federated enterprise. (*See explanatory note provided after meeting below.)

FIPS 201 and related suites of policy and standards document specifies using the same High-Assurance Identity Credential such as PIV, PIV-I, CAC, etc., for both physical as well as logical access control functions.

The Chairman referred the committee to a previous initiative to develop an airport credential based on the TWIC, the ACIS (in 2008). The Chairman agreed to upload the technical description to the committee AerOpus site.

Mr. Suneborn also reported on the emergence of devices which can be added to an existing HID reader with a to allow the reader to read multiple card types, including NFC. The Chairman pointed out the potential issues where multiple stacked IDs might provide conflicting signals. Dr. Branker noted that cyber security issues need to be coordinated as well.

FIPS 201-3 changes are still in the works "soon" after resolving 63 comments, including some proposed modifications for the PIN card data model. No change in security, it just adds operational capabilities.

Dr. Branker continues work on cyber issues across the entire document, including new NIST documents, European / UK (Brexit) issues -- most of which may turn out to be OK, but need to continue monitoring.

Mr. Hamilton continues to update the Biometrics section. He noted a recent conference in Washington, DC, on facial recognition and privacy issues which he will use to inform his section, and to coordinate with Mr. Zoufal to update.

Ms. Dores provided an update on her section, Facilitation. This section is delving into privacy and security control standards as well as some elements of risk management. Dr. Branker will assist.

This affects inbound traffic to CBP and access to their facilities, although it should be noted that passenger processing is peripheral to the RTCA scope. Facial recognition technology may eliminate some intermediate processes, controls, kiosks, but this needs to be coordinate with airport staff who must access those areas.

Ms. Dores will continue to address unresolved comments from Version K; some material will generally address Covid-pandemic issues, to be aligned with Mr. Zoufal's Credentialing section and Dr. Branker's Cyber section. There are likely to be significant changes based on a wide range of international travel concerns that currently remain in flux.

Mr. Kosatka raised the potential scope creep issue; further discussion generally agrees that this RTCA DO-230 document is to remain US focused but will likely include topics that surround pre-clearance, and various security and travel regulations from other countries.

Mr. Kosatka emphasized the underlying premise of RTCA DO-230 is primarily to address authorized access at the physical barrier or line_from public space to security-related space(s). It is not about CBP / INS access to the US through its borders, although DO-230 and the Security Guidelines document can support those issues in their approaches to airport security planning and design of areas affecting authorized operational access points.

8. Other Business

Ms. Ford is Chairman of RTCA SC-238. They are working on a document on Counter UAS tech standards. This engendered an extended discussion of security GA at airports and GA at commercial airports. Mr. Kosatka offers to discuss offline.

Mr. Kosatka noted a series of free online sessions on biometrics coming up in the EU. (**Info and registration links are included below.)

Dr. Wilkinson asked for potential volunteers for the Communications and Perimeter sections, as they are in need of leaders for the updates due mid-2022.

9. Schedule for future events

Oct 28th	80th Plenary
Dec 2nd	81st Plenary

10. Any Other Business:

There being no other business, the meeting was adjourned.

-S-
Art Kosatka
Secretary
CERTIFIED as a true and Accurate summary of the Meeting.

-S-	-S-
Christer Wilkinson	Alan Paterno
Co-Chairman	Co-Chairman

***Explanatory note by Lars provided after the meeting:**

The proposal is intended to simplify the creation of various level of access privileges, (for which specific authorization is required) creating a flexible, but standardized infrastructure that supports both generic access policies generated by an enterprise central authority, and also support local policies.

A significant step toward this goal is to define a library of Attributes/Roles for card holders. The Libraries of Attributes will be a time-consuming effort to create. They will need to be defined for each industry, say for example a bank teller who can move funds in/out of accounts – except their own. Logical access limits that authority. The next banker may be an Account Broker who have additional access and can also create new accounts as well as move funds between them. s and then a financial advisor with yet more privileges. The driver is from the logical access people more than the physical access groups, although there will be effects. My suggestion is going to be that a new, standardized Identity records is created (similar to the CHUID) but with one basic attribute and then two, or three more local attributes added. As an example, a medical doctor, may be allowed access to certain areas of a medical facility and also be allowed to access medical records. Further detail may include the ward the Dr is allowed to access. A similar tree is created to authorize access to medical records only for the specific set of patients. An Ophthalmologist may not access all records for Oncology cancer patients and so on.

Identity credential holders may then be pre-provisioned in an access control system automatically at the time of employment and issuance of the identity credential with certain basic access privileges for both physical and logical access. Local access control policies may then be accumulatively added to the individual card holder as required for the role. This is similar to current, legacy access control provisioning where administrators define access control points to areas of various departments of a facility and then creates an infrastructure to support grouping card holders to a set of departments. This is typically limited in some ACS system and more capability is required so just like the Logical Access Control systems have a very large set of privileges, the physical access control systems need to have a small, similar version. This will eventually be expanded with NGAC. Keep in mind, the Feds have for years deployed PACS in a Federated approach (as a server is a node on a federal network) and moved Identities around the network. The Attribute structure fit perfectly in these circumstances. If Mr. Smith is hired to the Accounting Department, Mr. Smith have automatically been pre-provisioned access to the Accounting Department areas and may us his card to enter. An expansion (or restructuring or better discrimination) of this concept is now underway. The final result will be more granularity, additional capability to add local access policies and of course to merge the similar structure for logical access to the NGAC system.

****Below are the referenced links and information for upcoming European sessions on biometrics**

Subject: Register Now for the Biometric Week - September 13 to 17

This year the Darmstadt Biometric Week is turned again into a Virtual Biometric Week. The organizing team is in preparation to run all events in the week in full virtual mode.

Please register *now* - separately for each event you plan to attend!

- The German Teletrust Biometric Working Group meeting on 2021-09-13:

https://urldefense.com/v3/__https://eab.org/events/program/220__;!!ETWISUBM!mSwP23tT2zbwRVWaPUXxcVKcnhEiJJaPN47p1fmQDbf04WzgMJijd5xJYUC3GG8Wdgrm1A$

- The EAB-RPC conference, from 2021-09-13 to 2021-09-15:

https://urldefense.com/v3/__https://eab.org/events/program/219__;!!ETWISUBM!mSwP23tT2zbwRVWaPUXxcVKcnhEiJJaPN47p1fmQDbf04WzgMJijd5xJYUC3GG8EoO5COQ$

- The EAB’s General Assembly (for members only) on 2021-09-13:

https://urldefense.com/v3/__https://eab.org/events/program/221__;!!ETWISUBM!mSwP23tT2zbwRVWaPUXxcVKcnhEiJJaPN47p1fmQDbf04WzgMJijd5xJYUC3GG91ngoJ8A$

- The final of the EAB awards on 2021-09-15:

https://urldefense.com/v3/__https://eab.org/events/program/222__;!!ETWISUBM!mSwP23tT2zbwRVWaPUXxcVKcnhEiJJaPN47p1fmQDbf04WzgMJijd5xJYUC3GG_hg-IEBA$

- The EAB’s Biometric Training Event on 2021-09-16 and 2021-09-17:

https://urldefense.com/v3/__https://eab.org/events/program/224__;!!ETWISUBM!mSwP23tT2zbwRVWaPUXxcVKcnhEiJJaPN47p1fmQDbf04WzgMJijd5xJYUC3GG-4lF8PLw$

- The 20th BIOSIG conference from 2021-09-15 to 2021-09-17:

https://urldefense.com/v3/__https://biosig.de/__;!!ETWISUBM!mSwP23tT2zbwRVWaPUXxcVKcnhEiJJaPN47p1fmQDbf04WzgMJijd5xJYUC3GG9nYKs9kA$