RTCA Paper No. 040-19/SC216-087
February 11, 2019

Summary of Forty-first Meeting

Special Committee 216 Plenary

Aeronautical Systems Security

The Forty-first Plenary of SC-216 was held February 4-5, 2019 at RTCA Headquarters, Washington, DC.

February 4, 2019

Attendees in the room:

- Dave Pierce (GE) – SC-216 Chairman
- Siobvan Nyikos (Boeing) – SC-216 Secretary
- Ed Hahn (Airline Pilots Association International)
- Karan Hofmann (RTCA) – SC-216 Program Director
- Mike Kelley (Esterline AVISTA)
- Marc Lord (Transport Canada)
- Sam Masri (Honeywell)
- Rebecca Morrison (RTCA)
- Ravi Nori (Teledyne)
- Ted Patmore (Delta)
- Mitch Trope (Garmin)
- Phil Watson (Panasonic)

Attendees on the phone:

- John Angermayer (Mitre)
- Claudio Castro (Embraer)
- Brian Daly (Transport Canada)
- John Flores (FAA)
- Raoufou Ganiou (Transport Canada)
- Cesar Gomez (FAA)
- Chris Grant (Collins)
- Clive Goodchild (BAE)
- Raoufou Ganiou (Transport Canada)
- Varun Khanna (FAA) – Government Authorized Official
- Marcus Labay (FAA)
- Kevin Meier (Cessna Aircraft Company)
- Stefan Schwindt (GE)
- Michael Severson (Bell Flight)

- Olivia Stella (American Airlines)
- Kevin Thomas (American Airlines)
- Brian Verna (FAA)
- Mohamed Waheed (Aviage)

Rebecca read off RTCA opening remarks

Introductions

<u>FAA remarks (Varun)</u>

We did not want security guidelines or regulations to go too far off, so we agreed to work with EUROCAE WG-72 on harmonization, checks and balances

AC drafted, but still in initial stages due to holidays and shutdowns

Mid to end of February – internal FAA review, get concurrences

Then it will go to industry

Rulemaking is parallel kickoff, several part 25 identified for rewrite

Not as extensive as part 23 rewrite, but 12-14 rules identified, keep new technology in mind

Brought up "2 for 1", if you want a new rule, you need to take out two

Rule will supersede special conditions

By next meeting, hoping to report on rulemaking

6 months from now for AC? Then the rule will follow

Marc – I thought administration said rule and AC must come out at same time?

Varun – AC can come out ahead of time, but not later

Clarification – still need special conditions until rule comes out

<u>December 2018 PMC and TOR Review (Dave)</u>

At PMC, discussed current state and proposed TOR revisions

WG-72 working four deliverables/activities, two of which are in SC-216 scope (ED-204A and ED-xxx information security event management)

SC-216 originally did not want to revise DO-355, but harmonization is priority

PMC approved revised TOR

Dave showed revised TOR

DFO -> GAR (Government Authorized Representative)

We (SC-216 and WG-72) are working as joint committees as far as these two deliverables in the TOR are concerned

SC-216 Coordination and Process

SC-216 and WG-72 leadership call in January to level set

Judicael Gros-Desirs (Airbus) and Frederique Dauvillaire (Thales) are on WG-72 Subgroup 3 leadership

Next WG-72 is week of March 18 at EUROCAE

Trying to get more presentations, feedback, etc. from airlines and operators, will continue to put out "help needed"

Stefan – clarification, regulations for safety-related

Phil – we already monitor, don't want to be on the hook to report non-safety, yes we need to think about propagation

Ted brought up ARINC 852

Siobvan – new info security event management document supposed to be more than 852, more than logging, can show the WG-72 scope during our working session

Dave – start with table of contents, assign to groups

Sam Masri (Honeywell) presentation

Safety incident reporting requirements

Monitor vulnerabilities that could be safety critical but have not led to an incident yet

Sources of info: customers, CERT, corporate, etc., want to add European sources in the future

Logic chain – is vulnerability valid? If valid, is it safety critical? Answer determines course of action

Valid + safety critical -> investigation

Safety org is separate from security org, true of industry and FAA

Challenge is to have a way to communicate between two organizations and become more effective

Reporting challenges include loss in confidence in the market

Stefan – touched on reporting to multiple authorities, use A-ISAC and ECCSA

Marc – Triage, what is a true security event, consider false positives and false negatives

Sam – Honeywell has a vetting process

Marc - Operator will need to involve OEM, supplier, and sub tier supplier at times, challenges there

Siobvan brought up EASA horizontal cybersecurity rule and Information Security Management System (ISMS) mandate, stretch goal is for ISMS and SMS to talk to each other

Stefan – allowed to take credit for activities performed elsewhere

Marc – does ISMS apply to operator or OEM?

Siobvan – everyone in aviation ecosystem, all of the above

Phil – regarding reporting challenges, yes concerns should be brought up to the A-ISAC

Karan – for US, can bring concerns to DHS

Varun – don't change current reporting aspects, but you may add to it

John Angermayer – intrusion does not always lead to safety event

Mitch – 80% of things we deal with are non-issues, 20% could not deal with right now, don't want to pipe that to the regulators, too much noise and counterproductive

Olivia – there are air carriers (not American) that don't have 24/7 monitoring, need something for all carrier sizes

Varun & Siobvan discussed logging and log analysis

Siobvan – there is a requirement to log, but that's it

Boeing has a team that is working log analysis

We don't get all the logs as that information is owned by the airlines, so how much we see and have to work with depends on individual partnerships with airlines

Hoping to work with more airlines on log analysis (so that we can detect and predict) as well as testing

Everyone is in agreement that it does not good to log if you don't do anything with the logs

Dave pointed out under forensics challenges, "refuse offers of help…from any unauthorized persons"

How do you put that in a document?

Ted – standardize items to look for in log files, then create tools, issue with data not being in the same format from aircraft to aircraft, filtering needed

Need help from DAH to deal with this

Ravi to Varun – in special conditions there were requirements about assets being layer protected, "automatically detected…"

Logging is one mechanism, what is expectation from FAA? Your interpretation of automatic?

Varun – no pilot action, written 10 years ago, some systems don't need to have it, architectural dependent

Cyber events will take form of denial of service of systems

Forensic, after the fact

Siobvan presented what WG-72 envisions as the scope of ED-204A and ED-xxx

WG-72 has been talking about not doing ED-xxx after all and merging those inputs into ED-204A, no decision yet

Siobvan's opinion – keep them two separate documents as we want to keep the scope of DO-355A tight and there is enough material to go into the new document

Stefan agrees

Need to discuss tomorrow when more WG-72 members are on the call

Ted brought up DO-355 chapters 8 and 10 – would those be moved to new doc?

Leave in and go into detail in new doc

Siobvan also presented another industry activity occurring this week, SAE Cyber Physical System Security (CPSS)

Stefan to present ECSCG tomorrow

Discussing operating rhythm and upcoming face to face meetings

Next ones should be week of March 18, June, and fall to meet industry needs

Marc – 3 ½ days is ideal

Dave brought up SC-216 working paper on this subject

Adjourn – team dinner

February 5, 2019

Attendees in the room:

- Dave Pierce (GE) – SC-216 Chairman
- Siobvan Nyikos (Boeing) – SC-216 Secretary
- Michael Davis (FAA, IT security)
- Ed Hahn (Airline Pilots Association International)
- Karan Hofmann (RTCA) – SC-216 Program Director
- Mike Kelley (Esterline AVISTA)
- Marc Lord (Transport Canada)
- Sam Masri (Honeywell)
- Rebecca Morrison (RTCA)
- Ravi Nori (Teledyne)
- Ted Patmore (Delta)
- Mitch Trope (Garmin)
- Phil Watson (Panasonic)
- Brian Verna (FAA)

Attendees on the phone:

- John Angermayer (Mitre)
- Claudio Castro (Embraer)
- Brian Daly (Transport Canada)
- John Flores (FAA)
- Raoufou Ganiou (Transport Canada)
- Cesar Gomez (FAA)
- Chris Grant (Collins)
- Anna Guégan (EUROCAE) – WG-72 Technical Programme Manager
- Judicael Gros-Desirs (Airbus) – WG-72 SG-3 chair
- Clive Goodchild (BAE)
- Brian Hoffman (ALPA)
- Ray Howard (SWA)
- Varun Khanna (FAA) – Government Authorized Official
- Nazih Khaouly (FAA)
- Marcus Labay (FAA)
- Kevin Meier (Cessna Aircraft Company)
- Cyrille Rosay (EASA) – WG-72 chair
- Stefan Schwindt (GE)
- Becky Selzer (United Airlines)
- Michael Severson (Bell Flight)
- Olivia Stella (American Airlines)
- Kevin Thomas (American Airlines)
- Mohamed Waheed (Aviage)
- Cameron Wright (SWA)

Review & approval of SC-216 Plenary 40 minutes

Anna – EUROCAE WG-72 needs to change their TOR so that this is a joint effort between SC-216 and WG-72

EUROCAE membership and policy statements, similar to RTCA

Note: Although we thought this Plenary session could be a joint Plenary session, since the call out notice was not published prior to the meeting on the EUROCAE side, this meeting is classified as an SC-216 Plenary session with WG-72 members invited to participate

Dave – SC-216 is in early phase, we need to learn what industry might need, then we will be more active

Judicael's WG-72 presentation

Judicael showed WG-72 structure to include subgroups and structure

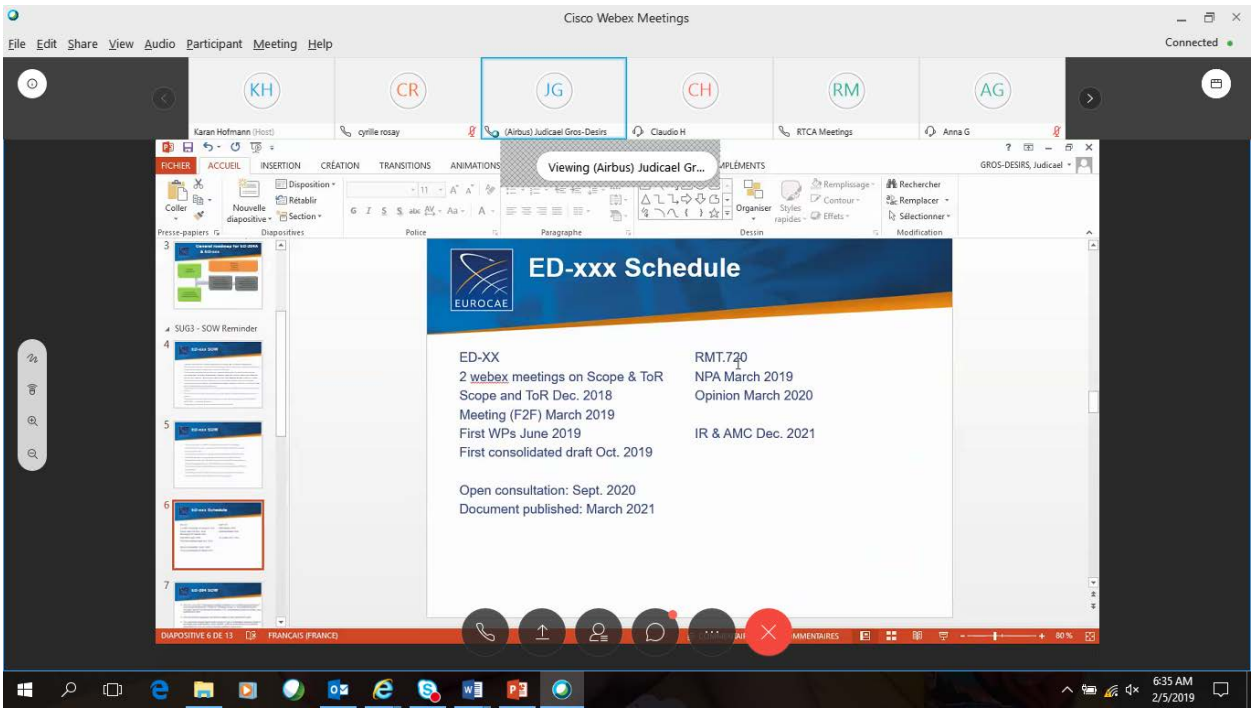
- SG2 -> ED-205
- SG3 -> ED-204A & ED-xxx
- SG4 -> ED-201A

Next WG-72 SG3 working group meeting planned February 13 (telecon)

Showed roadmap for documents, start with roadmap and synchronization

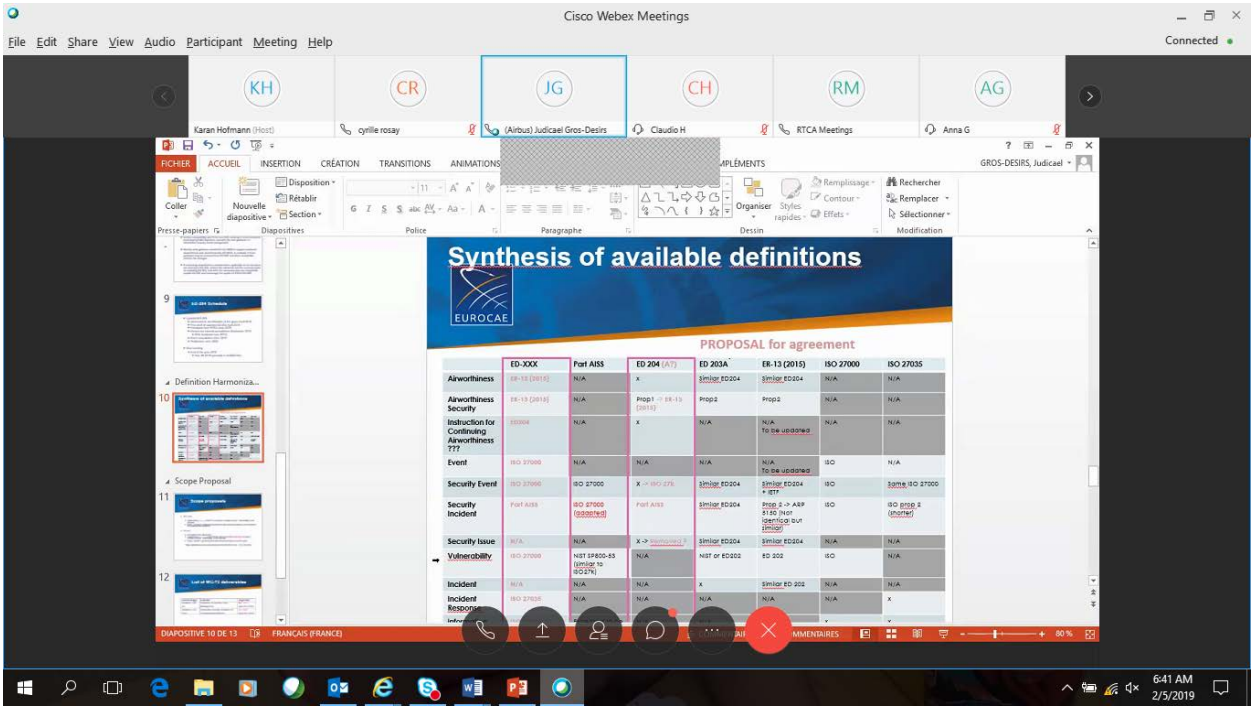
ED-xxx SOW, very close to what was recorded at WG-72 kickoff

Schedule for ED-xxx:



ED-204/DO-355 SOW, again, very close to what was recorded at WG-72 kickoff

Synthesis of available defintions – WG-72 created a matrix that maps definitions to EUROCAE secuirty documents to show gaps and disconnects



ED-xxx to be published March 2021

ED-204A to be published June 2020

Dave – SC-216 will need help understanding Aeronautical Information System Security (AISS) and how it applies to us

Varun – what is Part AISS?

Stefan - Part AISS is the outcome of EASA ESCP, “cybersecurity horizontal rule”

Some consider ESCP to be equivalent to ARAC

Anna - For March meeting, will schedule as much joint as possible in the afternoon so US can call in

Dave - Going back to slide on ED-xxx SOW, A-ISAC is great but doesn’t solve mandatory reporting problem

Mitch – also very expensive buy in

Stefan – ECCSA is mandatory and free

Should not specify a particular organization, rather state what is needed

Marc - Mandatory will be CA specific

Dave – consider sensitivity of information and distribution limits

Regarding bullet about ED-xxx covering whole life cycle…

Dave had issue with decomissioning part

Siobvan had issue with design part, design is taken care of via other documents (ED-203A), so perhaps scope should be edited and not be “whole life cycle, from design to decomisssioning”

Stefan – keep in mind ED-xxx is for more than just airplane, can include ground systems as well

Sam – will FAA delegate TSO?

Brian - No policy or guidance on how to gain that authorization

Marc - TCCA (Transport Canada) has no intention to delegate this to OEMs yet, when we do, it will be type design finding, not TSO

Siobvan presented Boeing position on scopes of DO-355A and DO-xxx

SC-216 and WG-72 agree with Boeing position:

- Priority is harmonization
- DO-355A/ED-204A
    - Scope should focus on post certification / continued airworthiness
    - Provide additional details needed for ANSP as an appendix to DO-355A/ED-204A so as not to revise the TOR or create an additional document
- Information Security Event Management
    - Overall, Boeing agrees with ED-xxx scope presented at WG-72 new activity kickoff in October
    - Need to take blue text from previous slides into consideration as this document is now being worked jointly with SC-216
    - Also add text from SC-216 working paper (originally meant for DO-355 revision) to new document

Some discussions during presentation…

Need to refer to ANSP as something generic and agreeable to US and Europe

Different operators turn in very different ANSPs

Varun stated that EASA / Europe is ahead regarding cybersecurity rulemaking and strategy with their ESCP in Aviation Cybersecurity

Marc asked if US ATM and ground services still considered to be government trusted services

Siobvan – yes, while WG-72 has ED-205, SC-216 still does not have an equivalent

Karan – whether or not we put out a document depends on members, not RTCA, now that we are reactivated we can revisit this area

Brian – until these services are privatized, FAA does not see reason to put out security guidance on ATM and ground services

Discussing log standardized format, common log aggregator

Varun - The more standardization you have, the less leyway you have in solutions

Ravi – took 2 years for ARINC spec, agreed on what goes into logs, but not format

Pressure from airline customers on analyzing logs, good tools out there, but there's a cost, hard for supplier to dictate what tool and how to approach, where to draw the line

Stefan – ECSCG

Purpose is to close gaps, avoid duplication of standards

Will be looking at regulations as well – where do we need standards, means of compliance

When rolling development plan published, Stefan will provide link

RTCA not involved, but they have partnership with EUROCAE

Dave – path forward

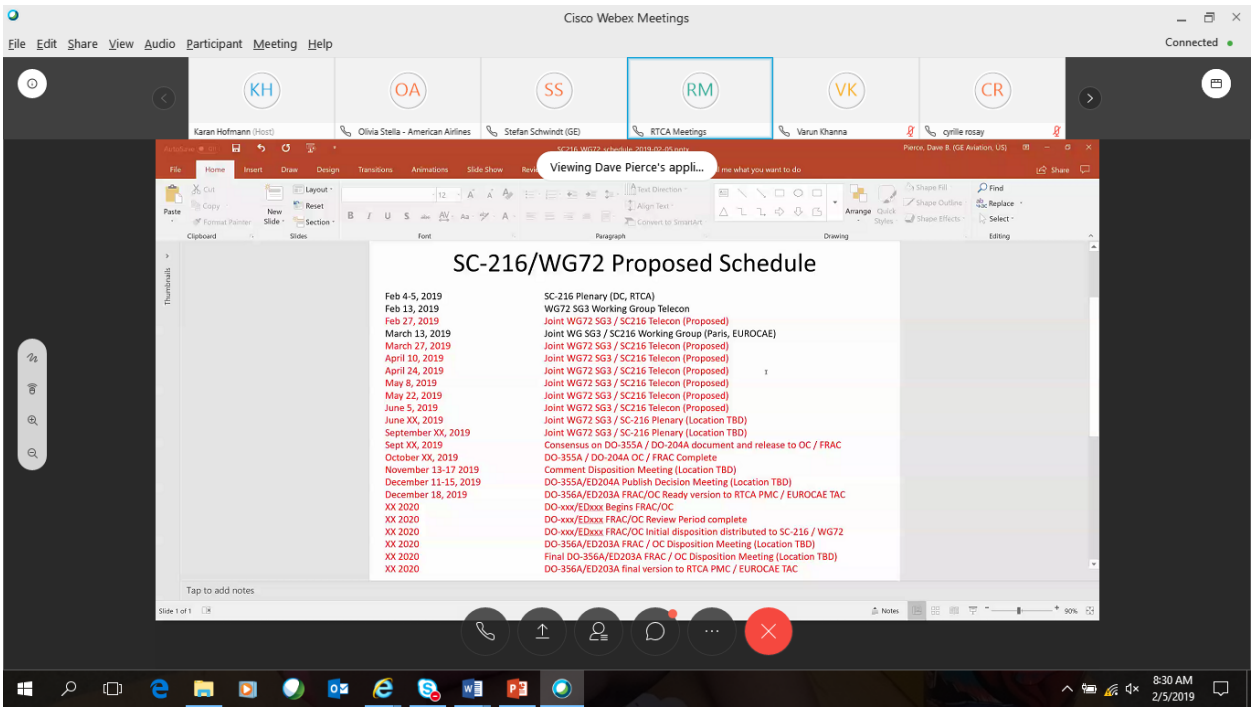
Biweekly telecons

- Definitions, scope
- Address ARAC ASISP and DO-356A material
- Determine next steps for content

Face to face

- SC-216 and WG-72 use results of each others' meetings for direction, work toward conent which can be alternatively discussed in each group and comments provided back to other committee
- Easier to have face to face for communication, but sometimes hard to travel
- Plan one face to face on each side, do we need this for DO-355A or just DO-xxx

Proposed schedule:



Dave – start with Siobvan's slides as they agree with Judicael's, baseline for working session

FAA, Transport Canada discussion

Again, no two operators are the same, no two manufacturers are the same

Lunch

NLT 2:30pm discussion schedule again

Dave showing Siobvan's slides to put more detail to them

Recommendation from SC-216 is Siobvan's slide 4 "green boxed approach", draw the line at certification where DO-356A is certification and DO-355A is post certification

ARAC ASISP -> DAH considerations put into 356A, so we can take them out of 355

Dave's paper + SC-216 discussions -> OK to leave in 355, but add wording to 355 chapter 8

Siobvan proposing to put that extra wording into new info security event management document

Regarding drawing the line at certification…

Marcus – what about STCs on airplane in service?

Mitch – changes still need to comply with 356A

Marc – same point of view, [STC] handled via certification process

Recommendation from SC-216 is STC treated as other certifications, need to follow DO-356A process

Siobvan – having said that, something to go into 355 or new document, would be nice if OEMs and aircraft manufacturers knew if a system was being STC'ed onto an already delivered airplane, need to have good communication between manufacturer and operator

Marc - Designer must supply continued airworthiness instructions, STC is required to produce ICAs

Dave - Validate that sufficient material has been generated for operational aspects, this needs to be in DO-355

Varun - Legacy systems into e-Enabled airplane, need to evaluate risk, implement controls if needed to prevent propagation of threat

Special conditions can and have been applied to an STC

Varun – IFE system – we don't care…unless it's a propagation issue

Better to have objectives than be perscriptive

STC – make sure it does not introduce any new risk to the airplane

Back to Siobvan's reccomendation to put Dave's wordding for 355 chapter 8 into info security event management document…

Reviewing wording

Also, what is the delineation between 355 and the new document

Recommendation from SC-216, delineate the two documents as follows:

DO-355 is preventative and deals with operational procedures for continuted airworthienss, what to do to prevent security events, in particular security events that can cause safety events

DO-xxx is reactive and deals with what to do if a security event occurs, if there is a safety impact, filtering, reporting, mitigation, how to put back into a safe and secure configuration (can apply to both airplane and IT systems)

Phil – more security notifications than just those related to airworthiness

Discussion of IMELs

Reviewing bullets that were supposed to go under 355 8.2.2.1

Stefan – throw in open source, supposed to be covered by commercial, but not everyone will recognize that, think DAL E systems with open source component or libraries

Varun – rarely have access to source or compiler library

In the process of editing the text, final text should be posted to the RTCA workspace

Recommendation from SC-216 - Need to come up with generic name for ANSP (since Europe doesn't use that term), make this normative and/or part of the main body to give it more strength, and work with customers to determine exactly what should go into this section to help them write their "ANSPs"

ANSP means something different in Europe

Ted - Aircraft Information Security Program (AISP)?

Marc – Information usually reserved for IT systmes

Aircraft Cybersecurity Program (ACP) or Aircraft Cyber Security Program (ACSP)

Decision - Aircraft Cybersecurity Program (ACP)

Dave action to format text from working paper and put it out as a proposal on the workspace

To partially address action, look at slide from Siobvan's presentation:

1. Ensure that data security protection is sufficient to prevent access by unauthorized devices or personnel external to the aircraft
2. Ensure that security threats specific to the certificate holder's operations are identified and assessed, and that risk mitigation strategies are implemented to ensure the continued airworthiness of the aircraft
    - Operators need to prove risk mitigations are in place
    - This is continued airworthiness, not certification – what process/methods should they use?
3. Prevent inadvertent or malicious changes to the aircraft network, including those possibly caused by maintenance activity
    - Operators want more guidance on how to validate passenger access as well as maintenance access
4. Prevent unauthorized access from sources onboard the aircraft
    - Airplane security design provides coverage, but operators want more guidance on wireless and cellular security

Also, look at Judicael's slides again

Need to agree on defintions

EUROCAE ER-013 is the glossary of terms they are using

Stefan – use ER-013 instead of define and re-define in each document, ER-013 should be master list

Difference between event and incident

Mitch – NTSB has specific meaning for incident

Siobvan reading from ED-203A/DO-356A: A security event is an action directed against a function with the intent to cause a security relevant change of state of the function. A security event may require investigation to check whether it was legitimate or unwanted. **An unwanted security event is a security incident.** A security event may be intentional or inadvertent

Clive – same as 204/355

Recommendation from SC-216 – use definitions of security event and security incident from DO-355 and DO-356A

Both ED-203A/DO-356A and ER-013 list both the NIST and 202A/326A defintions of vulnerability

Definitions are similarily worded

Recommendation from SC-216 – use the NIST and 202A/326A defintions of vulnerability

When does an event need to be reported? Discussion as opposed to defintion

Dave – take what currently exists and modify it?

Mitch – bar in Part 23 is very high

Internal company processes for handling field and in service products

Action to Varun with help from Stefan and Sam to come up with wording regarding security event, vulnerability, safety impacts, etc.

Before March meeting, would be good to have proposal for this and other actions / recommendations

Looking at third bullet on how info security event management includes detecting, logging, etc.

"Information security event management consist in detecting, logging, identifying, analyzing, scoring, documenting, reporting and reacting (including lessons learned) to an occurrence"

Look at items one by one

- Policy and procedures (NEW)
    - Ravi – add planning (policies and procedures)
    - Dave – policies can be tailored, procedures always needed
- Detecting
    - Dave - Do we need to detect every port scan?
    - Ted – qualify what we are detecting
- Logging
- Identifying
- Analyzing
- Scoring
    - Scoring refers to scoring severity of the event
- Documenting
- Reporting
- Reacting (including lessons learned)
    - Ed - Changes to ACP fall under reacting and lessons learned?
- Restore to a type design state (NEW)
    - Siobvan – add restore to safe and secure state
    - Marc – agree, but change to restore to type design state

Recommendation from SC-216 – add the following item to third bullet on ED-xxx SOW: policies and procedures, restoring system to a type design state, changes to ACP

Siobvan and Dave will clean up notes and send recommendations to WG-72 for their thoughts and SC-216 for “homework”

Next face to face March 19-22 at EUROCAE

Looking at next one after that June at RTCA – poll on RTCA workspace to figure out dates

Adjourn