Secretariat: MITA
1300 North 17th Street, Suite 900, Arlington, VA 22209, USA
http://www.dicomstandard.org/
dicom@dicomstandard.org
+1-703-841-3259

MINUTES

WORKING GROUP 14 Security

Date and Time	Tuesday 19 November 2019 11am-12pm US ET
Presiding Officers	Rob Horn, Producer Co-Chair Lawrence Tarbox, User Co-Chair
DICOM Secretariat	Lisa Spellman, General Secretary, DICOM

Voting Members Present	**Represented by**
Fairhaven Technologies	Rob Horn (Co-chair) (Voting)
GE	Matthew Hillyer (Voting)

Voting Members Not Present	**Represented by**
ACR	James Philbin (Voting)
Agfa	Bill Jacqmein (Voting)
Canon Medical Systems USA	Kevin O'Donnell (Alternate)
Canon Medical Systems	Scott Nitsche (Voting)
CFDA	Jia Zheng (Voting)
Change Healthcare	Elliot Silver (Alt voting) Roger Trevisan (Voting)
Hologic	Jeff Garrett (Voting)
JIRA	Akihiro Yomoda (Voting)
Konica Minolta Healthcare	Michael Laconti (Voting)
Laitek	Douglas Sluis (Voting)
MISAT	Chung-Yueh Lien (Voting)
PHC Co. LTD/JAHIS	Katsuya Watanabe (Voting
OFFIS	Marco Eichelberg (Voting)
Philips	Jeroen Medema (Alt Voting)
Philips	Ben Kokx (Voting)
PixelMed Publishing	David Clunie (Voting)
Siemens GmbH	Andreas Klingler (Alt Voting)
Siemens	Hans-Martin Von Stockhausen (Voting)
Siemens Healthineers	Mohammed Aleem (Alt voting)
Supersonic	Damien Lerat (Alt voting)
Stryker	Corey Cochran (Voting)
Univ. of Arkansas, Med. Sciences	Lawrence Tarbox (Co-chair) (Regrets)
Alternate Voting Members, Observers, Guests Present	
MITA	Lisa Spellman (WG Secretary)
MITA	Zack Hornberger (Observer)
MITA	Luiza Kowalczyk (Observer)
Philips	Nikhilesh Sonar (Observer)

1. **Opening**

1.1 Open the meeting and roll call.

1.3 Review of antitrust and patent rule.

1.3 Agenda review and approval.

1.4 We were unable to conduct a review and approval of minutes from 15 October 2019 since we did not meet quorum requirements. These minutes have been posted and will review on the next tcon.

2. **NCCoE comment review**

- Public comment closed 18 November. DICOM submitted comments and these are posted in today's meeting folder. Thank you, Rob, for doing all of the work on this and ExComm for a quick review.

3. **Any other new "hot issues" that have come up since the last WG-14 tcon?**

3.1 Pseudonymization: Rob reported a discussion from WG-06 Sex & Gender Task Group" regarding pseudonymization we got to looking at confidentiality profile and what to do about sex & gender and they might need some explanation since default will wind up labeling all patients as "non-binary"

- This topic needs some discussion from end-users of this data. Falls under security WG, start with an explanatory email to people that care about that issue first and then maybe a conference call
- Ask WG-06 & WG-10 to ask who are the right people to nail down this issue?
- **Timeline: Jan/Feb 2020**

3.2 There has been another cybersecurity conference with comments about DICOM, publishing document about *"…all of these products are full of holes…"* when people start looking, find products full of holes, so vendors need a good *"hole recognizing & hole filling process in place…"*

4. **MITA Cybersecurity update (Zack)**

- **Yarra Rules**: Will send to MITA Section for feedback – asked about some of the details for putting this into practice. Rob said he expected the volume of rules to be small – not many DICOM flaws to generate rules. Anyone doing Part 10 work, those rules do apply.
- **MITA White Paper:** Lisa spoke with Zack about WG-14's proposal and interest to see the MITA security related white papers to be updated.
- Both topics will be discussed at next MITA Section tcon on 11 December 2019 or January 2020

5. **Review of draft communications matrix**

- Lisa presented a rough draft. She will work with the chairs and WG-29 and present updated version on Dec or Jan tcon.

6. **Review of proposed updates to current DICOM-MITA white papers**

- The three existing white papers below were selected for updating at the 24 Sept tcon.
- The next steps to identify potential contributors.
- To be discussed on the Dec & Jan tcons.

Management of Machine Authentication Certificates

This paper helps healthcare providers and medical device engineering organizations decide how to use digital certificates to secure machine to machine communications.

- Perhaps we do this for DICOM. Do we note that people are not deploying TLS? Are they finding it too hard? And there could be other reasons as well.
- How many modalities have implemented TLS? It's on the laptop of the development engineers

Decision:

- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** The look must be updated across all documents.
- DICOM only or joint with MITA?
- Update: Rob found the original WORD of the published PDFs

Defending Medical Information Systems Against Malicious Software

This white paper informs both vendors (manufacturers and integrators of MedIS) and users (for example, hospitals and medical practices) about possible malware attacks and suggests ways to protect against them.

Decision:

- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** The look must be updated across all documents.
- DICOM only or joint with MITA?
- Anyone know where this WORD document is? July 8, 2003

Identification and Allocation of Basic Security Rules In Healthcare Imaging Systems

This paper identifies a set of security and privacy rules that, if properly enforced by healthcare providers or their medical imaging Information Technology (IT), can help them meet their legal obligations.

- The group also discussed this paper as a possible next update as well. Discuss on the 15 Oct call.
- MITRE has its "Att&ck Matrix. How about developing an "Att&ck Matrix" for DICOM?

Decision:

- **Content:** The group thinks the content for this document is mostly ok, but some updates are needed.
- **Look:** The look must be updated across all documents.
- DICOM only or joint with MITA?
- Update: Rob found the original WORD of the published PDFs
- Rob found the draft for approval but change between the draft and editorial. Things like footnotes and such. It would be nice. Dave Gobety (Kodal), Wolfgang (name). Rob will put them in the meeting folder.
- Doing these kinds of documents is supposed to be a joint JIRA, COCIR & NEMA all participating

<Action> Put this item in the WG-14 report for discussion at the RSNA DSC meeting on 2019-12-05.

7. NSA Manageable Network paper

- This has been discussed on several past calls. The proposal is for WG-14, jointly with MITA, to create a white paper based on NSA Manageable Network Plan . NSA created a high-level project plan. Add details about how to use DICOM and MDS2 to help fill in the gaps. MITA will help to produce and promote.
- Target audience: Hospital CISOs
- Link to draft: Rob Horn started a rough draft, is in Meeting Folder for 15 May 2019 (Note: DICOM does not list link to meeting folders in the Minutes).
- Link to NSA site: https://apps.nsa.gov/iaarchive/search.cfm?criteria=manageable+network+plan
- Status update: This was not discussed today, will be discussed again in early 2020.

8. Other general discussion notes for the development of shelf-ready content

- Tell a story about how it does through a story. The media wants the story to be 700 words or less
- Possible top questions/topics of no more than 700 words:
- *"Why doesn't DICOM include security?"* or "*What has DICOM done about Security?"*
- *" Hey administrator, have you looked at this…have you considered…?"*
- *"What to put in an RFP".*
    - It was noted that we will have to be thoughtful to ensure content does not stray into anti-trust territory. It is thought that we can include content that is general, but also helpful.
    - Maybe just include hyperlinks to sections
    - Call out the preamble, gives the mindset, intent – this could turn into a nice short piece

- **One pager checklist paper**: For administrators, including PACS and CISOs to include a short, focused list, a one pager/check-list for PACS Admins and only coming from the DICOM side (noting which may be DICOM-only and which may need to be DICOM-MITA jointly developed.
    - The content and goal is to aim end users at the **NSA Manageable Network** paper
    - Example: The real basics, Step 1: the real danger is connected to your network, many do not realize that they have holes, know your use case
- **NOTE:** We still need volunteers to take the lead on drafting these important documents.

9. Messaging/education opportunity: Possible session at RSNA20 to address recent critical security topics

- Idea: Submit a Course Refresher request, carry over to next agenda, maybe invite from NCCOE to co-present for RSNA 2020.

<Action> Lisa to find the date for RSNA 2020 submissions.

10. Digital Signature issue

- On hold for future tcons.

11. Expected Process activity, DICOM Section 8.4

- On hold for future tcons.

7. New Business/Old business

8. Next Meetings – tcons: (Usually the 3rd Tuesday, please note alternating times, 9-10am, 11am-12pm US ET)

Tue 17 December 2019: 9-10am US ET https://global.gotomeeting.com/join/686557661

Tue 21 January 2020: 11am – 12pm US ET: https://global.gotomeeting.com/join/435759061

10. Next Meetings - F2F

- None scheduled at this time.

11. Adjournment

The call adjourned at 11:30am US ET. Report prepared by Lisa Spellman, DICOM General Secretary. Report reviewed by MITA/NEMA legal counsel. CRS, November 22, 2019.

Appendix: Carry over information that we don't want to lose

Use of ACME certificates at Connectathons, IHE ITI profile proposal

- There was a discussion on January's call regarding ACME Certificates and other methods.
- A proposal was sent to Eric Poiseau, TM, European Connectathon and Steve Moore, TM, NA Connectathon. Steve and John Moehrke requested more info and pushed back a bit. They would like to better understand the need and value. Secure communications have not taken off (1) users don't know to ask for it (2) Vendors not pushing it

Next steps:

- Rob and Lawrence will do a bit more thinking and put together additional documentation.
- They might also draft a white paper. Continue discussion later in 2019.
- Lawrence has a presentation at SIIM2019 that will also cover some of this.
- Rob suggested that a good next step may be to draft a threat model to explain when and where it makes sense to use ACME. Perhaps also tie this to the MITRE ATT & CK model as well.