DICOM Secretariat/MITA

1300 North 17th Street, Suite 900

Arlington, VA 22209, USA

http://www.dicomstandard.org/

dicom@dicomstandard.org

Minutes

MEETING NAME WG-14

MEETING PLACE/DIAL IN GoToMeeting

DATE & TIME Tuesday, January 26, 2021, 9:00 AM - 10:00 AM EDT

PRESIDING OFFICERS Lawrence Tarbox, CHAIR, AAPM/Univ. of Arkansas for Medical Sciences

Rob Horn, CHAIR, Fairhaven Technologies

VOTING MEMBERS PRESENT

AAPM/UAMS	Lawrence Tarbox
Agfa	Bill Jacqmein
Fairhaven Technologies	Rob Horn
GE Healthcare	Matthew Hillyer
JIRA	Akihiro Yomoda
MISAT	Chung-Yueh Lien
PHC/JAHIS	Katsuya Watanabe
Siemens Healthineers	Hans-Martin von Stockhausen

VOTING MEMBERS ABSENT

Canon Medical Systems USA	Scott Nitsche*
Change Healthcare	Roger Trevisan*
Hologic	Jeff Garrett*
Laitek	Doug Sluis*
NMPA	Jia Zheng*
OFFIS	Marco Eichelberg*
Philips	Ben Kokx*
PixelMed	David Clunie*
Stryker	Corey Cochran*

OTHERS	Canon Medical Systems Europe	Keith Knight, Observer
	GE Healthcare	Steve Nichols
	MISAT	Tzu-Yun Ting, Observer
	Siemens Healthineers	Yufan Zhao
DICOM SECRETARIAT	Carolyn Hull, MITA	
	Zack Hornberger, MITA	

1 CALL TO ORDER AND REVIEW OF ANTI-TRUST RULES AND DICOM PATENT POLICY

The meeting was called to order. Staff reviewed the Guidelines for Conducting DICOM/NEMA Meetings and recorded attendance.

2 WELCOME/ATTENDANCE/INTRODUCTION

The attendance was taken.

3 REVIEW AND APPROVE AGENDA

The agenda was reviewed and approved.

4 REVIEW MINUTES

The minutes of the previous meetings – 12/22 and 11/17 were approved.

5 Hot issues that have come up since the last WG-14 tcon-

Security researchers being targeted by N. Korean Cyber operations to get leads into code, etc: https://www.zdnet.com/article/google-north-korean-hackers-have-targeted-security-researchers-via-social-media/

Sonic Wall was hacked-vulnerability in their software. Fix to firewall VPN. https://www.sonicwall.com/support/product-notification/urgent-security-notice-probable-sma-100-series-vulnerability-updated-jan-25-2021/210122173415410/

6. **Short paper (add)-conveying 1 time passwords over DICOM DIMSE- (Rob)-** Add this to the agenda for next call.

7. **NIST paper on PACS Security-**carryover from last month-discussion of potentially drafting a whitepaper. Suggestion to aim at midsize providers. Response from us, or possibility of a continuation of NIST. How can threat model DICOM could be an addition. Incorporating mitigations into threat modeling is important.

   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-24.pdf

Review for next month.

Someone tasked to draft – segmentation for medium-sized customers (no one).

8. **Zero Watermarking (article from Paul Sovelius):** https://link.springer.com/content/pdf/10.1007/s10278-020-00396-0.pdf

Reviewed article- no action.

9. **Certified time stamp CP2098-** (Rob)- came from Michael (?) updated definition of "certified timestamp."

   Will likely be reviewed in March and go into the voting packet. Action for the group: Please review if you are interested, and provide any comments.

10. **CP-2092_update_MAC_algorithms was approved for Voting Packet (i.e. public comment).** This mostly adds SHA-3 family of MAC algorithms. It also refactors some common text into one table (to help the Sup223 Inventory) and fixes some typos. Review and comment.

Will likely be reviewed in March and go into the voting packet. Is it worth it to write new profiles?

Draft a supplement. Will discuss whether want to deprecate existing in favor of new.

11. **Digital signatures profile to incorporate SHA-2**-Discuss and vote whether to add more profiles. Discuss during next meeting, add to next meeting agenda.

12. **Consulting companies pushing DICOM security issues-** Did not discuss, add to next meeting agenda.

13. **Follow up from DSC meeting/Bryan Fang from CIMICS conversation: WG-14 to explore ideas to prevent information sent by a modality from being intercepted and tampered with**. Discuss next time.

14. **MITA Update: Collaborative white papers**

14.1. **Whitepapers:** Discuss how to present these on DICOM website and come up awith a few ideas.

Development of shelf-ready content-

This project still holds a high priority as it's important for DICOM & MITA to have these resources.

- Concept description:
- Develop a series of short documents – stories – around 700 words that can be posted on DICOM website as FAQ-type info and able to send to have these short pieces at the immediate ready when some issue blows up and media and others request written feedback with an ASAP timeline.
- **Audience**: These are not meant to be technical engineering papers. These are something a product manager or a regulator would read. ~700 words is about the length of an opinion piece, be able to give to media and use in an FAQ.

Topic / Title	Content to be included	Lead
"Why doesn't DICOM mandate security"	- Possible content: DICOM is not a regulatory body - Not always the best fit solution for a particular organization	Rob
"How can I tell if my system is exposed?"	- We describe how to do it.	Hans v on tcon 2019-12-17
"*How to turn on encryption and why"*	- Different for modalities and PACs	Hans v on tcon 2019-12-17
"How an administrator could use SHODAN to find leaks"	- "You've heard about all of those exposed DICOM ports, you can find out if any of yours are exposed at your institution. Enter info into Shodan & it will tell you the open ports and IP addresses..." - Can be tricky if have dynamic IPs and such, but at least give them guidance	**Please review the draft. For next time (Sept meeting), how do we want to package these? Internally when something comes up. Creating a section on the website.**
"Hey administrator, have you looked at X / have you considered…?"	- DICOM is not responsible for the deployment. We don't want to come across as defensive, rather, explain what the reader can do	
"What to put in an RFP".	- Ensure content doesn't stray into anti-trust territory. We think we can include content that is general, but 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	- Audience: For administrators, including PACS and CISOs. - 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 are to aim end users at **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 - **Status**: The WG started a draft on the call (2019-12-17).	

6 Profile/standardizing a user authentication scheme, re: 2FA.

7 NSA Manageable Network paper

- **Action item**: Add in a section to the same white paper talking about NSA. A new document web security considerations. Then, if people want to do DICOM 2.0, can go further. Add to table. Will be looking for a volunteer.

- 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:**

8 DATE AND TIME OF NEXT MEETINGS

The next face to face meeting and any teleconferences of the committees can be proposed.

Tuesday, February 23, 2021, 9:00AM ET

Tuesday, March 23, 2021, 9:00AM ET

12. ADJOURN- The meeting adjourned at 10:07AM ET

Submitted by: Carolyn Hull, 2/2/21

Reviewed by Counsel 2/3/21

NEMALINK CODE 09-wg14

SUBMITTED BY	Hull, Carolyn
SUBMITTED ON	1/28/21
LEGAL REVIEW	2/3/21
UPLOAD LOCATION	Enter upload location.