International Association of Drilling Contractors

Advanced Rig Technology

Cybersecurity Subcommittee

05 May 2016

IADC
10370 Richmond Ave., Suite 760

Houston, TX 77042

Attendance

Name		Company Name
Marco	Ayala	**AE Solutions**
Chris	Boylan	**DNV GL**
Clifford	Donald	**GE Oil & Gas**
Cris	DeWitt	**ABS**
Erlend	Engum	**NATIONAL OILWELL VARCO**
Robert	Frandsen	**Maersk Drilling**
Christopher	Goetz	**Kingston Systems**
Tom	Horan	**Rowan**
Hamed	Hamedifar	**DNV GL**
Siv Hilde	Houmb	**Secure-NOK**
Mike	Killalea	**IADC**
Terry	Loftis	**Transocean**
Trenton	Martin	**Transocean**
Robin	Macmillan	**NATIONAL OILWELL VARCO**
Melissa	Mejias	**IADC**
Nathan	Moralez	**BP**
Richard	Parliman	**Lloyd's Register Energy-Drilling**
John	Powell	**AE Solutions**
Steven	Ronan	**Northwest Technical Solutions**
Nina	Tvedt	**Noxa DA**

International Association of Drilling Contractors

Agenda for the meeting:

1. Welcome and Introductions

2. Review of Antitrust Guidelines and Facility Orientation

3. Review of Minutes from Last Meeting

4. Orientation on DHS / US Coast Guard / NIST activities on cybersecurity – Melissa Mejias (IADC)

5. Risk Assessment Example

6. AOB

Minutes:

1. Welcome and short introduction of the participants – “round around table”.

2. Meeting delegates was reminded of the IADC antitrust guidelines.

3. Minutes from the subcommittee meetings are posted at: http://www.iadc.org/advanced-rig-technology-committee/meeting-minutes/. There were no comments to the minutes from the last IADC ART Cybersecurity Subcommittee meeting(March 9, 2016).

4. Orientation on DHS / US Coast Guard / NIST activities on cybersecurity – Melissa Mejias (IADC)

Melissa Mejias is a Legislative Analyst with IADC. Ms. Mejias have compiled a list of activities and initiatives of relevance to cybersecurity for drilling assets from the following entities: DHS, NIST, US Coast Guard, API, European Union, US Legislation, Industry Groups and IMO. The list will be revised in collaboration with the subcommittee.

DHS:

- Draft voluntary standards for ISAO (Information Sharing and Analysis Organization). The goal is to define a standard to enable sharing of cybersecurity information across all types of organizations, also those beyond traditional critical infrastructure sectors. The initial set of information sharing standards is expected published June 2016.
    - It is worth noting that the National Offshore Safety Advisory Committee (NOSAC) in their response to the US Coast Guards on the eight (8) questions that would assist USCG in developing policy to help vessel and facility operators identify and address cyber-related vulnerabilities that could contribute to a Transportation Security Incident (TSI) published in the Federal Register on December 18, 2014, by the USCG, recommended that reporting of cybersecurity information would be voluntary minimum reporting, and with one common instance to report to. Currently, there are many different initiatives on cybersecurity reporting across DHS, ICS CERT, US Coast Guards and more.
    - The decision made by the meeting was to engage with the API and to advocate for voluntary minimalistic reporting standards and that reporting be coordinated and directed to one common official entity. Note that the NOSAC response to the US Coast Guard proposes to use a simplified version of the reporting schema used by the ICS CERT.
- Cyber-Data Repository. The DHS and its Cyber Incident Data and Analysis Working Group (CIDAWG) has put forward a proposal of cyber-data repository that is open for public comment until May 24, 2016. More information: https://www.federalregister.gov/articles/2016/03/28/2016-06856/national-protection-and-programs-directorate-national-protection-and-programs-directorate-seeks. The IADC members are encouraged to review and comment. IADC with

Melissa Mejias will monitor the progress of this activity and report to the Cybersecurity Subcommittee.

- Please refer to the enclosed list of activities for additional information on DHS and relevant cybersecurity activities.

US Coast Guard:

- NIST organized the NIST Cybersecurity Framework Workshop April 6-7, 2016, at the NIST headquarters in Gaithersburg. During this workshop the US Coast Guard participated in two sessions: a panel debate on the Bulk Liquid Transfer Cybersecurity Framework Profile and the collaboration with the industry and NIST; and a session presenting the Bulk Liquid Cybersecurity Framework Profile. In the panel debate, Capt. Verne Gifford represented the US Coast Guard. A summary of the questions and answers from the US Coast Guard can be found here: http://mariners.coastguard.dodlive.mil/2016/04/15/4152014-nist-cybersecurity-framework-shop/. Representing the US Coast Guard during the session discussing the Bulk Liquid Transfer Cybersecurity Profile were: LCDR Josh Rose and LT Josephine Ann Long. There were also representatives from the NIST and the NIST NCCoE, who has developed the profile in collaboration with the US Coast Guard. What is worth noting is that the US Coast Guard have plans to develop a Cybersecurity Profile for MODUs and that this profile will be based on the Bulk Liquid Transfer profile. What is also worth noting is that LCDR Josh Rose has been active in communicating with the NOSAC during the development of their response to the 8 (eight) questions from the US Coast Guard (see above for more details).
- The meeting decided to develop guidelines for minimum cybersecurity requirements for drilling assets based on the NOSAC document. The intension of the guidelines is to compile a minimum requirement set that the Subcommittee can use to engage with the US Coast Guard for comments and considerations.
- Melissa Mejias was tasked with keeping the Subcommittee updated on the relevant activities of the US Coast Guard and especially the work on the cybersecurity profiles.
- Please refer to the enclosed list of activities for additional information on the US Coast Guard and relevant cybersecurity activities.

US Legislation:

- Regarding the Energy bill addressing cybersecurity in electricity section. There are mounting pressure on Capitol Hill to create a regulatory framework for addressing cyber issues through data breach notification and other federal legislation.
- Melissa Mejias was tasked with keeping the Subcommittee updated on the advances of this activities on Capitol Hill.

API:

- Cyber component of SEMS. API and COS have expressed interest in including IADC in drafting a cyber component in SEMS. The meeting agreed that this is something that the IADC should be involved in. Melissa Mejias will act as the IADC liaison with API regarding cybersecurity matters. The cyber component of SEMS will be further discussed at the next Subcommittee meeting.
- Cybersecurity Deference Policy Program. A one-page white paper will be made available for review in June. The meeting decided to review the white paper when it is published. Melissa Meijas is to inform the Subcommittee through the Subcommittee meeting on the progress of the white paper. The white paper is scheduled for discussion at the July 7 Subcommittee meeting.
- Cyber Safety. API and COS (and possibly IADC) to lead a cyber safety subgroup. This will focus on IT system resilience and human factors other than threats from outside actors (i.e. threats caused by inside actions). The scope for this workgroup will be to determine policy positions for our industry regarding the integrity of digital controls of offshore operations, especially to respond to increased interest by the Department of Interior Bureau of Safety and Environmental Enforcement (BSEE) and the US Coast Guard on this topic. The scope for this workgroup is not exactly cybersecurity. Rather, it is about the integrity of digital controls more broadly. What the API and COS are looking for are representatives for this workgroup from IADC member companies that have responsibility for making sure that cyber systems work properly and that any

risks are reduced that could produce a safety or environmental incident. The first task for this workgroup is to produce a one-pager that describes the industry's management of risks on this topic.
- The meeting decided that the IADC should participate in this work. Melissa Meijas was appointed the IADC liaison to API. Melissa Meijas and Siv Hilde Houmb will coordinate and discuss with Aaron Padilla, API, regarding this activity and report back to the Subcommittee at the next Subcommittee meeting July 7, 2016.

Others:
- The ONG SCC membership will vote to include IADC as a member of the ONG-ISAC on May 23. Melissa Meijas is in dialog with the ONG SCC leadership and the ONG-ISAC Executive Director regarding this matter.

Summary of decisions made by the meeting:
- Melissa Meijas was appointed the IADC liaison to API.
- Melissa Meijas was requested to keep the Subcommittee updated on relevant cybersecurity activities from: DHS, US Coast Guard, US Legislation, API and others.
- The Subcommittee to work on a Guidelines for Minimum Cybersecurity Requirements for Drilling Assets. The first draft tentatively scheduled for review by the Subcommittee at the meeting July 7, 2016, and the guidelines to be published September 2016.

5. Risk Assessment Example.

Deferred to next meeting.

6. AOB. The subcommittee meetings are announced on the IADC website. Please remember to register. The meeting calendar for the IADC ART Cybersecurity subcommittee for 2016 are the following:

- July 7, 2016
- September 1, 2016
- November 3, 2016

Updated and tentative schedule of deliverables for the IADC ART Cybersecurity Subcommittee:
- September 2016 – Guidelines for Minimum Cybersecurity Requirements for Drilling Assets.
- December 2016 - Guidelines for Network Segmentation.
- December 2016 – Cybersecurity Training v1.0.
- June 2017 – Guidelines for Hardening of Control Systems.
- December 2017 – Guidelines on Security Monitoring and Audit.

There were no other business and meeting adjourned.

Action Points:

AP no.	Description	Responsible	Deadline
01	Top 10 threats for Drilling Assets.	Part of AP 02.	TBD and dependent on AP 02, as the review of the top 10 threats is part of the risk assessment example discussion.

02	Risk assessment of generic Drilling Asset applying the IADC Guideline and ISA/IEC 62443-3-2.	Siv and all.	First round of assessment completed and presented at Jan 21 meeting. The risk assessment result will be discussed and revised in the July 7 meeting.
03	Network Segmentation standards and best practices.	Part of AP 02.	First iteration completed Sept 4, 2015. The network segmentation discussion is part of the risk assessment example discussion (see AP 02).
04	Evaluate alternatives for collecting and publishing relevant cybersecurity information (vulnerabilities, top 10 threats, etc.)	Siv and Linda Hsieh (coordinate with Mike Killelea)	July 7, 2016
05	Develop block diagram or similar of Drilling Asset (expand on the diagram used for the risk assessment example (AP 02))	John Jorgensen and Siv	TBD
06	Develop training materials for risk assessment and management	Greg, Wesley and Siv	TBD
07	Distribute risk assessment example result to subcommittee participants	Siv	Done
08	Guidelines for Minimum Cybersecurity Requirements for Drilling Assets	Siv and all	First draft July 7, 2016
09	Communicate and coordinate with API regarding Cyber Safety	Melissa Meijas	July 7, 2016

Appendix (next page)

IADC Cyber Strategy –items for consideration.

Party		Summary of Activity - Regulation/Legislation/Initiative	Date	Remarks
DHS	Draft 'voluntary standards' for ISAO	The draft guidance will include specific questions to be addressed: "What needs to be considered by a newly-forming ISAO and what are the first steps? What capabilities might an ISO provide? What types of information will be shared and what are some mechanisms for doing so? What security and privacy is needed for a newly forming ISAO? What mentoring support is available for newly forming ISAOs? What government programs and services are available to assist ISAOs? What concerns do regulators and law enforcement have about the new ISAO construct?"	DHS announced April 21st in the Federal Register that the "initial set of standards' for creating information sharing and analysis organizations will be released for comment in June.	**IADC action item: Monitor and await comment. Coordinate with API on if/how industry should get involved.**
	Cyber-Data Repository	The creation of a national repository for submitting and analyzing information about cyber breaches was the focus of an April 19-20 meeting hosted by the DHS and its Cyber Incident Data and Analysis Working Group, or CIDAWG, where there seemed to be a consensus on the role of a non-governmental group in long-term management of the proposed data system. During the two-day meeting, industry officials were asked for input on the design and operation of the proposed repository, which insurers support as a way to provide actuarial data on cyber risk and trends.	DHS is accepting public comment on a proposed cyber-data repository until May 24th.	**As this may likely be an Operator driven process in the future, the drilling contractors need to cooperate. IADC Draft minimum requirements that drilling contractors should meet for contracting evaluation.**
	DHS reports to Congress on Cyber directorate reorganization	On March 17th, DHS submitted a report to Congress titled "Cyber and Infrastructure Protection Transition Way Ahead." The report provides details on a plan to transition from the National Protection and Programs Directorate to the Cyber and Infrastructure Protection Agency, an effort to improve operational focus ad internal coordination of the agency's cyber initiatives.		
	Info-sharing guidelines for privacy, civil liberties	The guidelines from DHS and Justice provide interim procedures for protecting privacy and civil liberties when conducting cyber threat information sharing under CISA. The document offers guidelines for receipt, retention, use, and dissemination of cyber-threat indicators.		API is monitoring and receiving updates through the Chamber of Commerce. **IADC action item: continue monitoring**
NIST	NIST 800-160 standard: Cyber guide offering 'holistic' security approach for IT engineers	The guide aims to help IT engineers build cybersecurity controls into their systems and mapping them to international standards and business processes. The standards offer companies a way to approach cyber issues		http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf

		across the spectrum, tackling supply chain, acquisition security and other topics.		
	Cybersecurity Framework Workshop 2016	Specific panel presentations addressed framework use, international alignment, cyber insurance, and state and local issues. In addition, there were special topics discussions on issues including the cyber assessment tool produced by federal financial regulators, and issues in the maritime sector and related Coast Guard activities.	NIST is expecting to issue a report in mid-May on the outcome of the workshop meeting and the next steps for the framework	**Currently no report has been released.**
	Special publication 800-150 Guide to Cyber Threat Information Sharing	The revised document removes pieces that were seen as distracting from the core elements of the guidance, including a discussion on information exchange architectures and the maturity of an organization's cybersecurity practices. The revised draft expands on the discussion of cyber threat indicator sharing and restructures the section on privacy and sensitivity. The Guide is designed for computer security incident response teams, systems and network Administrators, security staff, privacy officers, technical support staff, CISOs, CIOs, computer program managers, and other stakeholders in cyber threat information sharing activities.	The revised draft is open for public comment.	
USCG	Bulk Liquid Transfer Cybersecurity Framework Profile	The Profile will map the NIST Cybersecurity Framework to the maritime bulk liquid sub-sector. The USCG described it as a voluntary assessment tool that the maritime industry will ideally use to start a cyber risk management program or more mature organizations will request their	The Coast Guard hopes to expand its framework profile work to other maritime sub-sectors, starting with offshore drilling, and passenger vessels and terminals.	The USCG is working with API and AFPM to coordinate testing of the Profile. The USCG would like IADC"s assistance testing the NIST CSF MODU profile once drafted. No timeline has been provided for the MODU profile at this time. The USCG is also working with FERC to perform cyber architecture reviews at LNG facilities. Lessons learned from this mature compliance regime will help to inform how the USCG will hope to promote cyber risk management in the maritime

				community. **IADC will independently begin working on the MODU Cybersecurity framework profile for the USCG. IADC (Melissa) will liaise with the USCG (LCDR Rose and LT Long) that upon sufficient review it may be accepted.**
Int'l Regs.	European Union Data Rules	Lawyers in Europe and the US are advising clients to get ready for implementation of EU data protection rules and the recently unveiled Privacy Shield agreement, despite uncertainties about the legal viability of these requirements and the details of how these two data regimes will work together.		The Chamber of Commerce is actively working on this issue on behalf of API and other industry members. **IADC action item: continue monitoring**
US Legislation	Cyber investigators	Sen. Sheldon Whitehouse (D-RI) is planning to introduce legislation soon with bipartisan support to strengthen Justice Department authority to investigate and prosecute cyber attackers.		
	Energy bill addressing cybersecurity in electricity sector	On April 20th the Senate passed the Energy Policy Modernization Act, a comprehensive energy bill that contains provisions to improve the cyber posture of the U.S. electric grid. The bill contains language giving the DOE greater authority over electric grid cyber incident response and shielding cyber threat data from public disclosure. A controversial amendment offered by Sen. Susan Collins [R-ME] requiring assessments of the grid industry's cyber posture failed to make it into the final bill. Industries urged lawmakers to block the amendment noting that it contradicts the voluntary nature of the cybersecurity bill that was signed into law in December.	The bill must be reconciled with a House measure.	Pressure is mounting on Capitol Hill to create regulatory frameworks for addressing cyber issues through data breach notification and other federal legislation.
	The Cybersecurity Act of 2015	On Dec. 18th President Obama signed the Cybersecurity Information Sharing Act as part of an omnibus spending package for fiscal 2016.		
	Senate Homeland Security panel to focus on Critical infrastructure cybersecurity	The Senate Homeland Security and Government Affairs Committee will hold a hearing to assess the security of critical infrastructure, with industry officials. Committee Chairman Ron Johnson (r-WI) and ranking member Tom Carper (D-DE) announced Monday that the hearing will specifically examine critical infrastructure threats, vulnerabilities, and solutions to national security threats.		Scheduled to testify are Tom Farmer, chairman of the Partnership for Critical Infrastructure Security; Koppel, author of *Lights Out: A Cyberattack, a Nation*

				Unprepared, Surviving the Aftermath; and Scott Aaronson, managing director of cyber and infrastructure security at the Edison Electric Institute.
IMO	Measures to Enhance Maritime Security	MSC 96/4/3 Proposals for guidance on maritime cybersecurity – this document provides information on national regulations published by China and provides proposals for guidance on maritime cybersecurity. (China)		
	Measures to Enhance Maritime Security	MSC 96/4/1 - MEASURES TO ENHANCE MARITIME SECURITY, The Guidelines on cybersecurity on board ships (ICS, IUMI, BIMCO, INTERTANKO, CLIA and INTERCARGO)		
	Measures to Enhance Maritime Security	MSC 96/4/2 - MEASURES TO ENHANCE MARITIME SECURITY, Guidelines for Cyber risk Management (Canada, Japan, Liberia, the Marshall Islands, Norway and United States)		
	Measures to Enhance Maritime Security	MSC 96/INF.4 - MEASURES TO ENHANCE MARITIME SECURITY, Measures aimed at improving cybersecurity on a ship (France)		
Industry	Information Sharing and Analysis Organization (ISAO) draft plans on "immediate issues"	April 25th was the deadline for ISAO working groups to submit their draft plans for immediate steps in creating cyber threat-indicator exchanges. Subgroups include privacy and security; support; capabilities; and government relations.	The ISAO group expects to issue draft standards for comment in June, according to a recent Federal Register notice, and expects to finalize those standards by September.	
	Information sharing and Analysis Organization (ISAO) draft of long-term plan for cyber info-sharing	The ISAO process is intended to spur the creation of info-sharing groups in response to evolving cyber threats that transcend industry sectors and geographic regions, and to build on the current information sharing and analysis center, or ISACs, that focus on specific critical industries. The working groups are made of government and private-sector representatives, including layers and critical industries.	The plan by the ISAO standards organization is expected to be made available for six-week public comment period at the beginning of May. The document will coincide with the release of draft plans by six working groups on "immediate issues" to be dealt with in getting the ISAO process up and running.	

	Cyber component of SEMS	API and COS are currently looking at the cyber component in SEMS to get ahead of a possible BSEE regulation (i.e. Well Control Rule – RTM and software vulnerabilities)	API and COS are interested in our level of interest and willingness to get involved in drafting a cyber component in SEMS.	It there would be a new regulation, what would that look like? How long would it take for IADC to stand up a committee to draft a standard? **IADC Cybersecurity Committee is already working on guidelines addressing the cyber component in SEMS. IADC will coordinate efforts with API to ensure views align and efforts are not duplicated.**
	Cybersecurity Deterrence Policy Program	API and the Chamber of Commerce are working on a one-page policy paper.	The one-page white paper will be available for review in June.	
	Cyber Safety	API and COS (and possibly IADC) to lead on a cyber safety subgroup. This will focus on IT system resilience and human factors – other than threats from outside actors.		IADC to determine the level of engagement with API and COS. **IADC member companies will participate. A list of member companies will be submitted to API in due time.**
Upcoming Scheduled Meetings/ Forums	Annual U.S. Maritime Industry NIAG and CSO Meeting	Topic: Cybersecurity in the Maritime Domain Host: Primary-National Maritime Intelligence-Integration Office, along with the Maritime Administration's Office of Maritime Security, USCG Office of Vessel Compliance Keynote Speakers: Senior Leadership from the Federal Maritime Commission, Maritime Administration Administrator Mr. Paul "Chip" Jaenichen or Deputy Administrator Mr. Mike Rodriguez, additional speakers TBD Audience: Company Security Officers and company IT or management personnel from the Deep Sea, Offshore Service and MODU Communities, along with selected port personnel	Dates: 19-20 July 2016 (2 days) Times: 0830-1600	
	AFPM - Q&A and Technology Forum	The American Fuel & Petrochemical Manufacturers will hold their 2nd annual AFPM Cybersecurity Day on Monday, September 26, in Baltimore, Maryland.	AFPM is looking for presenters and panelist who have experience in one or more of the areas listed in their call for papers. If you have an abstract you would like to submit, please visit the AFPM website and complete the online submission form.	If you have an abstract you would like to submit, please visit the AFPM website and complete the online submission form