International Association of Drilling Contractors

Advanced Rig Technology
Cybersecurity Subcommittee
15 February 2018
IADC
10370 Richmond Ave., Suite 760
Houston, TX 77042

Attendance

Name		Company Name
Donald	Crouch	**LLOYD´s Register Drilling Integrity Services**
Michael	Edwards	**BP**
Siv Hilde	Houmb	**SECURE-NOK**
Michael	Lewis	**Chevron**
Robin	Macmillan	**National Oilwell Varco**
Melissa	Mejias	**IADC**
Jeff	Melrose	**Rowan Companies**
Juan	Negrete	**Rowan Companies**
Ben	Ramduny	**Seadrill**
Alan	Spackman	**IADC**
David	Zacher	**ONG-ISAC**

Agenda for the meeting:

1. Welcome and Introductions
2. Review of Antitrust Guidelines and Facility Orientation
3. Review of Minutes from Last Meeting
4. Update on Legislative and Standardization Activities
    a. NVIC
    b. Offshore Profile
    c. Senate Bill, S.2083: Strengthening Cybersecurity in our Information Sharing and Coordination in our Ports of 2017
5. IADC Cybersecurity Guidelines Development – Network Segmentation
6. ONG ISAC – Walkthrough of their information sharing process and handling using the NotPetya malware as an example
7. AOB and close of meeting

International Association of Drilling Contractors

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 November 16, 2017 IADC ART Cybersecurity Subcommittee meeting.

4. Update on Legislative and Standardization Activities from Melissa Mejias
The meeting did not review the update due to time constraints. The summary is therefore provided in the minutes. Please review and note the activities on the new senate bill **S. 2083.**

IADC Cybersecurity Overview – February 2018

IADC Cybersecurity Subcommittee.

- **Guidelines.**
    - IADC's ART Cybersecurity Subcommittee issued "IADC Guidelines for Assessing and Managing Cybersecurity Risks to Drilling Assets" March 2016.
    - IADC's ART Cybersecurity Subcommittee issued "Guidelines for Minimum Cybersecurity Requirements for Drilling Assets" January 2018
- Other guidelines under development:
    - Guidelines for Network Segmentation – to be completed April 2018
    - Cybersecurity training – focusing on risk assessment and management – to be completed June 2018 – Volunteers needed to help draft the guidelines
    - Guidelines for hardening of control systems focusing on existing drilling assets (to include patching) – to be completed June 2018 – Volunteers needed to help draft the guidelines
    - Guidelines for security monitoring and audit – to be completed December 2018
- **API-IADC Joint paper.** API and IADC have drafted a joint paper on Cyber Risk Management of the Industrial Control Systems in the Offshore and Onshore Oil & Natural Gas Industry. This paper is intended to inform policy-makers as regulators and others having concerns regarding cyber security in the industry. The audience is the USCG and the policy drivers are the USCG policy making for maritime operations, focused primarily on ICS cybersecurity. The joint paper was finalized July 2017.
- **API, IOGP, and IADC Joint position paper on cybersecurity:** The audience is the EU Commission, MEPs and EU member state national-level policy makers; US Congress and US White House. The policy drivers are the EU NIS transposition by EU member states and any potential new laws or Executive Orders in the US covering cybersecurity generally. The position paper has not been finalized.

The next IADC Cybersecurity meetings are workshops are scheduled for

- 12 April: IADC Cybersecurity Workshop (Stavanger, Norway)
- 6 June: IADC Cybersecurity Subcommittee meeting (Houston, TX)

DHS/USCG.

- **Offshore Operations Profile**. On 12 January 2018 the U.S. Coast Guard posted the updated Cybersecurity Framework Profiles document with the additions of the Offshore Operations (and Passenger Vessels). The USCG will attach these guidance documents to future Navigation, Vessel, and Inspection Circulars (NVICs). You can find the blog post and instructions for assessing the files here: http://mariners.coastguard.dodlive.mil/2018/01/12/1-12-2018-release-of-offshore-operations-and-passenger-vessel-cybersecurity-framework-profiles/
    - The next profile will focus on navigation & automation for vessels and facilities. It is currently pending contract review.

- **NVIC.** The Coast Guard issued a notice in the Federal Register on July 12 requesting comments on the draft Navigation and Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risk at Maritime Transpiration Security Act (MTSA) Regulated Facilities. This NVIC proposes to clarify the existing requirements under MTSA to incorporate analysis of computer and cyber risk and guidance for addressing those risks. The comment period was extended 30 days from original due date of 11 September 2017. IADC submitted comments on October 11th.
  - USCG received 256 comments and has reviewed them all. Current stage is they are implementing actionable comments, which includes meeting with other CG offices to see how best to incorporate some of the items. The updated draft should be completed in the near future – no specific timeline. As of current, they are looking to remove enclosure 2 (the source of many of the issues in the comments).
    - To note, only 24 comments have been posted in two different dockets.
  - The National Maritime Security Advisory Committee (Task 17-02) has been tasked with providing views on the NVIC, and their timeline for doing so extends into this year. As such, IADC is working with the NMSAC to provide input to the Coast Guard in order to influence their thinking regarding the proposed NVIC.

- **US – DHS Cybersecurity information sharing needs improvement.** A new report from the Department of Homeland Security's Inspector General on the Department's implementation of the Cybersecurity Act of 2015 has concluded that "DHS has developed adequate policies and procedures and the capability to share cyber threat indicators and defensive measures. Additionally, DHS has properly classified the indicators and defensive measures and accounted for the security clearances of private sector recipients of this shared information." However, the report states that "Despite meeting these requirements, the Department faces challenges to effectively sharing cyber threat information across Federal and private sector entities. Given that NPPD (National Protection and Programs Directorate) emphasizes timeliness, velocity, and volume in cybersecurity information sharing, the system DHS currently uses does not provide the quality, contextual data needed to effectively defend against ever-evolving threats. Without acquiring a cross-domain information processing solution and automated tools, DHS cannot analyze and share threat information timely. Further, without enhanced outreach, DHS cannot increase participation and improve coordination of information sharing across Federal and private organizations." NPPD has concurred with the report's recommendations and has implemented corrective actions to address the findings.
- LCDR Josephine Long has started phasing out of her position at the Office of Port & Facility Compliance (CG-FAC) at Headquarters. LCDR Brandon Links is the new POC.
- Tentative meeting scheduled for the week of March 12 to meet with the USCG and NCCoE NIST to go through the new IADC guidelines on Minimum Cybersecurity Requirements for Drilling Assets.

ONG-ISAC. In early February 2017, IADC joined the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) and now has access to this shared pool of intelligence on cyber incidents, threats, vulnerabilities, and associated responses. The ONG-ISAC recently signed a multiyear agreement to use ThreatConnect as its threat intelligence platform, which broadens the collaborative community.

- IADC will work with the ONG-ISAC to formulate a plan to best communicate information, alerts, and notifications received from the ONG-ISAC to members.
- Educational webinar - The ONG-ISAC will host an educational webinar. The Agenda & date are still tentative. ONG-ISAC webinars are strictly educational and there is no sales pitch involved. Webinar topics are based on ONG-ISAC member request (examples: ONG insider threats, ONG vendor vulnerabilities, etc.).

International Association of Drilling Contractors

Information Sharing Remote Secure Video Teleconference
DOE is working to improve the way it shares classified threat information with cleared industry representatives and is looking to test its ability to host remote secure video teleconferences (SVTC). If you are interested in participating in this effort in the coming months, please email Siv Hilde Houmb or Melissa Mejias.

GOMEX. Gulf of Mexico Cyber Exercise (GOMEX) at BSEE's office in New Orleans on 8 August. The one day table top cyber exercise was planned for port and maritime stakeholders and coordinated between the Maritime and Port Security Information Sharing and Analysis Organization (MPS-ISAO), the Department of Homeland Security's National Cyber Exercise and Planning Program (NCEPP), and the USCG Outer Continental Shelf Division with their Area Maritime Security Committee's Exercise Team. Industry and regulators came together for a planned incident - disruption via spear phishing - for lessons learned. IADC had six member companies participating. Please contact Siv Hilde Houmb or Melissa Mejias if you would like a copy of the key take aways.

CSO/NMIO/NIAG meetings. On January 17th the National Interagency Advisory Group (NIAG) hosted a cyber threats meeting at the National Maritime Intelligence Center in Washington, D.C. Topics included:

1. National Security Council discussed their perspective on a possible cyber policy that would mirror OPA 90.

IOGP Security Committee. At the last committee in November the group voted to focus primarily on physical security and will refrain from engaging in cyber related efforts. The next committee meeting is scheduled for **25-26 April 2018 in London, UK.**

- IADC sent out an announcement to members on July 24th requesting comments on the IOGP-API Position Paper on Cybersecurity. Note, IADC joined the position paper. Draft has not been finalized.
- API-IOGP Cybersecurity Europe Conference for the Oil and Natural Gas Industry: A call for presentations is available here: http://www.api.org/products-and-services/events/calendar/2018/cyber-europe. The conference will be held **27-28 June, 2018 in London, UK**.

ONG SCC. On **11 December in Washington, D.C.** the ONG SCC held its third educational session at DOE on physical and cybersecurity. Last September the ONG SCC held its first educational session which provided a brief overview of the how the industry works – from production to distribution. The second provided a layout of the regulatory framework for the industry. Siv Hilde Houmb and Nathan Moralez presented on cyber security on behalf of the upstream sector.

The last ONG SCC meeting for the year will be held on **5-6 March in Washington, DC**.

IMO. MSC 98 Summary Notes from 7-16 June. *Measures to Enhance Maritime Security Guidance on Maritime Cyber Risk Management – Working Group Issue reflected in 98/WP.9* MSC 96 approved MSC.1/.Circ.1526 on *Interim Guidelines on Maritime Cyber Risk Management* with the Committee (98) superseding these interim guidelines via an MSC-FAL.1Circ.[…] titled *Guidelines on Maritime Cyber Risk Management.* The committee noted advice from the Legal Division that cyber risks could be addressed as part of the existing provisions of ISPS and ISM. Though some delegations thought mandatory provisions are necessary, they agreed these guidelines would further consideration after more experience could be gained from use of the guidelines.

Additionally, the working group considered MSC 98/5/2, the U.S. paper calling for the need to address cyber risk within the context of ISM. Several interesting points were made in the working group and plenary discussion:

- Why make a specific reference to an element already considered part of an overall strategy for addressing risk?
- Why ISM and not ISPS?
- Why identify a date for "entry into force" (first DOC renewal after 1 January 2021), will doing so be potentially misleading to some administrations?
- Isn't it important to address cybersecurity concerns before 1 January 2021?

Discussion of the date went back and forth in plenary, but the Committee finally adopted the resolution (annex 1) with the date included.

Congress.

- **H.R.3101:** Strengthening Cybersecurity Information Sharing and Coordination in our Ports Act of 2017. The legislation passed legislation in a voice vote on 24 October 2017 that would instruct DHS to take steps to boost cyber information sharing and coordination at US ports in reaction to a "notPetya" attack at the Port of Los Angeles. On 25 October 2017 the bill was sent to the Senate Commerce, Science and Transportation committee

  IADC's position – We would like to influence the shape of the Bill rather than fight it.
    - In December Nathan Morales and Siv presented at a DOE educational session on cybersecurity in the ONG sector here in Washington, DC. While here we took the opportunity to voice our concerns on H.R. 3101 and S.2083 with Sen. Dan Sullivan, the cosponsor of the Senate Bill and the committee where the Bill currently resides, the Senate committee on Commerce, Science, and Transportation. In short, IADC is not in support of the bill as it is written. Points of concern are listed below. The Senate committee has been visited by several trade associations and does not plan to move the Bill forward until the concerns raised by industry have been corrected. IADC will continue to work with the committee and the Coast Guard to make sure the Bill does not move forward until the Bill has been amended.
        - Change title to reflect facilities and vessels, too – let's just call it what it is: covers all maritime jurisdiction of Coast Guard
        - Section 1: Should state: "…Secretary of Homeland Security*, working through US Coast Guard*, shall…."
        - Section 2, Part 4: We'd prefer to flip this on its head and have guidelines be to clarify how US Coast Guard will share, e.g., from Coast Guard National Response Center (NRC) to NCCIC (and on to private sector) – that this bill should task the development of guidelines that would prompt the Coast Guard to figure out how NRC and NCCIC work together and how the Coast Guard will work with industry
        - Section 2, Part 5: include (G) ISACs and ISAOs – This section request the NMSAC to make recommendations to the Secretary (of Homeland Security) on enhancing information sharing between the federal agencies, however, it fails to mention ISACS and ISAOs.
        - Primary concern is that it creates duplication in roles and assessment tools between DHS and the USCG.
            - On February 8th the trades received updated language from the USCG Fellow on the Senate Committee on Commerce, Science, and Transportation prior to the meeting with Sen. Harris and Sen. Sullivan's staff on February 8th. Updated language attached.

- **H.R.3359:** Cybersecurity and Infrastructure Security Agency Act of 2017
    - Passed House on 11 December 2017, Introduced 24 July 2017
    - ***Summary***: This bill amends the Homeland Security Act of 2002 to redesignate the Department of Homeland Security's (DHS's) National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency (CISA) to be

headed by a Director of National Cybersecurity and Infrastructure Security to lead national efforts to protect and enhance the security and resilience of U.S. cybersecurity, emergency communications, and critical infrastructure.

CISA shall be composed of DHS components reorganized as: (1) the Cybersecurity Division; (2) the Infrastructure Security Division; and (3) the Emergency Communications Division, which was previously the Office for Emergency Communications. The agency will also have a privacy officer to ensure compliance with relevant federal laws.

CISA must carry out DHS's responsibilities concerning chemical facilities antiterrorism standards.

This legislation would rename the NPPD and bind the department's cyber and physical mission and create new director-level position at the agency that reports directly to the DHS. It would help achieve a long standing goal of DHS officials to create a stand-alone operational organization and cyber and infrastructure.

- Senate hearing on 7 February 2018, Homeland Security and Governmental Affairs Committee: Reauthorizing DHS: Positioning DHS to Address New and Emerging Threats to the Homeland
  - Reorganization of the DPP was addressed.

Administration.

- **President Trump's budget Proposal.** Cyber spending escapes budget cuts in Trump's proposal. 77 agencies now have a line item for cyber spending. DHS will only receive a slight uptick in cyber money. Most would go toward boosting the operational budget of the agency's main cyber wing, the NPPD.

- **CSER.** On 14 February 2018 a press release was issued by Secretary Perry announcing the formation of a new Office of Cybersecurity, Energy, Security, and Emergency response (CESER). "The CESER office will be led by an Assistant Secretary that will focus on energy infrastructure security, responsibilities assigned to the Department and report to the Under Secretary of Energy".

Industry Document/Standards & Guidelines.

- **International Standard Organization (ISO).** New document: ISO/IEC 27000:2018 – *Information Technology –Security techniques – Information security management systems—Overview and vocabulary*. This document replaces ISO/IEC 27000:2016
- **DNV.** New cyber guidance from DNV: DNVGL-CP-0231 Cyber security capabilities of control system components (Type approval)

Dates for the calendar:

1 March: InfraGard NCR Annual Member meeting (Washington, DC)
6-7 March: ONG SCC: Industry-Government Meeting (Washington, DC)
12 April: IADC Cybersecurity Workshop (Stavanger, Norway)
25-26 April: IOGP Security Committee meeting (London, UK)
6 June: IADC Cybersecurity Subcommittee meeting (Houston, TX)
19-20 June: ONG SCC: Industry-Government Meeting (National Lab, TBD)
27 June: API-IOGP Cybersecurity Europe Conference for the Oil and Natural Gas industry (London, UK)
9 August: IADC Cybersecurity Subcommittee meeting (Houston, TX)
24-25 August: AFPM Security Conference (New Orleans, LA)
11 October: IADC Cybersecurity Subcommittee meeting (Houston, TX)
13 December: IADC Cybersecurity Subcommittee meeting (Houston, TX)

5. IADC Cybersecurity Guidelines Development – Network Segmentation
Ben Ramduny (Seadrill) and Nathan Moralez (BP) gave an update on the status of the network segmentation guidelines. The guidelines are expected to be in a final state (ready for formal review) April 2018. To aid in the development of the network segmentation guidelines, there will be an interim review process which will be organized in March 2018 with a 2-week comment period. This will include all relevant IADC members, but especially the appointed interim review group. This group is comprised of: Felipe Mondragón (Noble), Ernesto Espinoza (MHWirth) and Juan Negrete (Rowan Companies).

6. ONG ISAC – Walkthrough of their information sharing process and handling using the NotPetya malware as an example.

David Zacher, Executive Director of ONG-ISAC, joined the meeting to discuss ONG-ISAC and how it operates, including the benefits for its members, and to provide a walkthrough of how ONG-ISAC and its analysts, in collaboration with its members, identified and addressed the NotPetya malware. The meeting delegates learned details on the ONG-ISAC operational process in the case of critical cyber malware and attacks and how this particular malware was addressed in practice. Additional information both on ONG-ISAC and the NotPetya malware is available upon request from David Zacker at: dzacher @ ongisac.org.

7. AOB and close of meeting. The subcommittee meetings are announced on the IADC website. Please remember to register. The next subcommittee meeting is April 12 in Stavanger, Norway. This is a full-day workshop, free of charge. Please remember to register.

The subcommittee is seeking co-chairs and would like to recruit two co-chairs: one representative from drilling contractors and one representative from operators. Interested candidates should contact Siv, Robin or Melissa.

Updated and tentative schedule of deliverables for the IADC ART Cybersecurity Subcommittee:

- July 2018 - Guidelines for Network Segmentation.
- September 2018 – Cybersecurity Training v1.0.
- December 2018 – Guidelines for Hardening of Control Systems.
- December 2018 – Guidelines on Security Monitoring and Audit.

There were no other business and meeting adjourned.

The annexes to the minutes are:
Annex 1: Ports Cyber Bill (S. 2083.)
Annex 2: IADC´s comments to S. 2083.