IADC Cybersecurity Overview – July 2017

IADC Cybersecurity Subcommittee.

- **Guidelines.** IADC's ART Cybersecurity Subcommittee issued "IADC Guidelines for Assessing and Managing Cybersecurity Risks to Drilling Assets" Other guidelines under development:
    - Guidelines for Minimum Cybersecurity Requirements for Drilling Assets
    - Guidelines for Network Segmentation
    - Cybersecurity training – focusing on risk assessment and management
    - Guidelines for hardening of control systems focusing on existing drilling assets (to include patching)
    - Guidelines for security monitoring and audit
- **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 paper is scheduled to be finalized in July 2017. API and IADC have an upcoming conference call to discuss changes to the document in July before the next IADC cyber subcommittee meeting.
- **The next IADC Cybersecurity meetings are scheduled for 14 September and 16 November**

USCG/NIST/MITRE – Cyber Frameworks.

- **Cybersecurity Framework Profile for MODUs**. The Coast Guard is working with the National Institute of Standards & Technology (NIST) and industry to develop Framework Profiles various for the maritime industry sectors. The first Profile for "bulk liquid transfer" has already been issued. Work on a MODU Profile was initiated in late-January with the cooperation of IADC's ART Cybersecurity Subcommittee; however, during the course of this work, the Coast Guard determined that the work scope needed to be expanded to the broader offshore oil and gas industry. IADC hosted a kick-off meeting for this effort in January at the IADC office. IADC continues to assist NIST in drafting the MODU portion of the profile.
- **Offshore Operations Profile**. On 1 June 2017 the US Coast Guard (USCG) published a blog post requesting comments on the on-going Offshore Operations Profile work. The deadline for comments was 15 June 2017; however, the USCG has extended the deadline by two weeks. IADC sent an announcement to members requesting comments. IADC submitted comments on June 13, 2017.
- **NAVIC.** The Coast Guard issued a notice in the Federal Register on July 12 requesting comments on the draft Navigation and Inspection Circular (NIVIC) 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. IADC will send an announcement to members requesting comments. **Comments are due September 11, 2017**.

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.

- In May the ONG-ISAC submitted their first DrillBit update to Amy. They will continue to submit articles every two months or as needed.
- Within the next few weeks IADC will work to formulate a plan to best communicate information received from the ONG-ISAC to members.
- **Educational webinar** - The ONG-ISAC is hosting an educational webinar in August, 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.)

GOMEX. Gulf of Mexico Cyber Exercise (GOMEX) at BSEE's office in **New Orleans on August 8th**. This one day table top cyber exercise is planned for port and maritime stakeholders and is being 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 will come together for a planned incident - disruption via spear phishing - for lessons learned. IADC has six member companies participating.

CSO/NMIO/NIAG meeting. The next Company Security Officer (CSO) meeting is scheduled for **September 20th in Galveston**, Texas at Texas Maritime Academy. This event also counts as the National Maritime Intelligence-Integration Office's (NMIO) annual Maritime Industry National Maritime Interagency Advisory Group (NIAG) meeting. This forum combines industry, government and academia to analyze global threats in the maritime domain. In the past this event has been held in Washington, D.C. The meeting will be held at the Texas Maritime Academy in Galveston to encourage industry attendance.

IOGP Security Committee. IADC, API and IOGP met in London during the API Cybersecurity European Conference in June to discuss whether IOGP would be able to take on the task of leading the definition of cybersecurity requirements from the operators. There seems to be some interest in this, but it will take some time. IADC, API and IOGP were each given the opportunity to present their organization and their efforts in cybersecurity at the conference. Siv spoke on behalf of IADC. Siv has also been invited to join the IOGP security committee, which will take on cybersecurity in as a topic. The next meeting is scheduled for **November 13-14 in Houston, TX.**

- IADC sent out an announcement to members on July 24th requesting comments on the IOGP API Position Paper on Cybersecurity.

ONG SCC. On June 13 & 14th the ONG SCC held a meeting in Knoxville, TN at the DOE National Labs. The first day was an industry only meeting. Most of the discussion focused on issues not relevant to the drilling contractors (i.e. drones and pipeline); this is because there is a lack of participation from the upstream sector. IADC is their only upstream member, aside from API who represents upstream, midstream, and downstream. I recommended the SCC reach out to and invite other upstream trade associations.

The next meeting is scheduled for **August 15 & 16th in Washington, D.C.** Before the next meeting the SCC will look into having NIST update the Cybersecurity Risk Management Tools survey - last updated two years ago. Once updated the trades will send the survey to member companies for their feedback. I do not believe IADC member companies participated in the last survey.

On **November 8th or 9th** the ONG SCC plans to hold its third educational session at DOE on Cybersecurity. Last September the ONG SCC held its first educational session which provided brief overview of the how the industry works – from production to distribution. The second provided a layout of the regulatory framework for the industry.

The last ONG SCC meeting for the year will be held in **Houston on 5-6 December**.

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.

Executive Order 13800. On May 11, 2017, President Trump issued Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," to improve the Nation's cyber posture and capabilities in the face of intensifying cybersecurity threats to its digital and physical security. DHS is pleased to announce the first update on the implementation of EO 13800. This update and future updates can be found on the United States Computer Emergency Readiness Team (US-CERT) EO 13800 website. Below are a couple of highlights from the EO 13800 update.

- **Request for Comments** - On June 8, the National Telecommunications & Information Administration (NTIA) issued a Request For Comments (RFC) on Promoting Stakeholder Action Against Botnets and Other Automated Threats. Comments are due on or before **5 p.m. EDT on July 28, 2017**.
- **Workshop** - The National Institute of Standards and Technology (NIST) has also announced a cross-sector, participatory workshop to accompany the Request for Comment. The workshop is designed to allow stakeholders to explore a range of current and emerging solutions to enhance the resilience of the Internet against automated, distributed threats. Information on that workshop is available on the Enhancing Resilience of the Internet and Communications Ecosystem website. Registration for the workshop is now closed.
  July 11-12; National Cybersecurity Center of Excellence; 9700 Great Seneca Highway, Rockville, MD
  For workshop questions, please contact Kevin Stine, kevin.stine@nist.gov.

INFRAGARD. DHS seeking topic submissions for 2018 Analytic Exchange Program - deadline July 28th. The Department of Homeland Security, Office of Intelligence and Analysis, Private Sector Engagement team, on behalf of the Office of the Director of National Intelligence, is planning for the launch of the next cycle of the

Public-Private Analytic Exchange Program (AEP) and is soliciting UNCLASSIFIED topic ideas for AEP 2018 from our partners.

The AEP provides government and private sector analysts the opportunity to work together on joint research projects that will allow them to engage and collaborate on issues affecting national and homeland security. Throughout a six month program year, participants will work together on virtual teams to create joint analytic products of interest to both the private sector and the U.S. government. Please see the one page flyer for more information on the program and its outcomes.

This year's AEP has been very successful and rewarding for its participants, and they would like to request your participation in influencing the next AEP cycle by proposing unclassified topic ideas for next year's team projects. The 2016 project abstracts and list of 2017 topics describe some of the previous projects.

If you would like to propose your own topic(s) for the upcoming year, please submit this form and return it to AEP@hq.dhs.gov by July 28, 2017. Please feel free to submit multiple topic ideas. Should you have questions, please contact program manager Tammy Padilla.

Tammy Padilla
Program Manager, Public-Private Analytic Exchange Program
Office of Intelligence and Analysis, Private Sector Engagement
Department of Homeland Security
202-447-3338 Desk | Tammy.Padilla@hq.dhs.gov| trpadilla@dhs.ic.gov

Dates to put on the calendar:
ONG-ISAC – Educational Webinar - TBA
Gomex – August 8 (NOLA)
NVIC Comments due September 11
IADC Cybersecurity committee meetings – September 14 and November 16 (Houston)
CSO/NIMO/NIAG meeting – September 20 (Galveston)
ONG SCC Educational Session for DOE – November 8 or 9th (Washington, DC)
IOGP Security Committee meeting – November 13 -14 (Houston)
ONG SCC Meeting – December 5-6 (Houston)