Terms of Reference – OGUK Special Interest Group

Group Name:	**Service Organisations Cyber Security Forum**
Group Type:	Special Interest Group
Chair: **Vice Chair:**	Andrew Thom (Wood) TBD
Issue Date	January 2020

Rationale & Objectives

The objective of the forum is to provide an active body through which representatives from O&G service companies can collaborate on Cyber Security, the purpose being to provide a robust and coherent strategy against the ever-evolving security threat landscape.

The forum will:

- Provide a leadership role within the O&G Service sector for cyber/information security
- Liaise with other industry bodies to share best practice specifically:
- Operators Special Interest Group.
- Oil & gas UK
- Oil and Gas Technology Centre
- Promote security skills development in the industry working with universities etc and providing placements for students.
- Identify opportunities to collaborate and support other supply chain organisations
- Act as SMEs for the industry to advise and enable on security initiatives
- Review new technology and consider joint industry projects to further secure the supply chain activities
- Provide support and guidance to the HOIT Forum
- Set up and lead special workgroups to address specific concerns of the Forum members
- Collaborate with information sharing and incident response in the event of a security incident within the sector by:
- Proactively sharing threat intelligence
- Establishing best practice in Cyber Security
- Sharing information regarding latest security solutions and technologies

The Service Organisations Cyber Security (SOCS) Forum shall operate in a fully transparent, proportionate and non-discriminatory manner and work towards addressing identified security issues within the scope described above. The collection and/or sharing of any information amongst its members as well as all correspondence and dealings shall be subject to Oil & Gas UK's Competition Law Compliance Policy[1].

The SOCS Forum shall seek to proceed by consensus. Where there is no consensus the matter will be raised to Oil & Gas UK (and ultimately its Chief Executive) for determination.

---

[1] See: https://oilandgasuk.co.uk/wp-content/uploads/2015/04/OGUK-Competition-Law-Policy-September-2015.pdf

Terms of Reference – OGUK Special Interest Group

Membership

A senior manager with responsibility for security, from every member of the group will be nominated to take part in the forum. The expectation is that each company nominates a suitable manager to participate in the Forum, engages constructively, and steps up to support the group's aims or individual work groups as required.

One representative for each member should try to attend each meeting. Multiple representatives should be avoided unless there is a specific topic of relevance on the agenda. Members may be asked to dedicate time to the work of the SOCS Forum (or any of its work groups) from time to time, and this may be during working hours.

The forum chair and vice chair reserve the right to remove members that do not actively participate in the forum's activities. Whilst more members are welcome the goal of the forum is to collaborate and share information for the benefit of all. As such if an organisation consistently missing meetings and fails to participate they may be removed from the forum. This will only be done as a last resort and after discussion with the organisation to ascertain if the forum processes can be changed to aid participation.

Non-members may be invited to attend part of a SOCS Forum meeting to present or discuss particular topics where those organisations have a relevant contribution or expertise; however they will not have a right to participate in the making of decisions of the SOCS forum.

New members will be welcomed to the group but must meet the following criteria:

- The proposed member plays a significant part in the supply chain to Operators/Licensees of the UKCS energy industry.
- The proposed member's primary business is not the provision of information technology hardware, software, services, or consultancy.

Should a dispute arise regarding whether a potential member meets the criteria above, this will be determined by the Forum Chair and Vice Chair, in consultation with OGUK, who will ensure that membership criteria are applied fairly in compliance with competition law. In such an event the reason for admission or rejection will be documented on in the minutes of the next meeting for future reference.

The forum will have 3 additional members from non-supply chain organisations, who will assist in threat intelligence sharing, forum administration, and other specialist tasks:

- OGUK
- UK Government National Cyber Security Centre (NCSC)
- Oil & Gas Information Security Forum (OGISF)

Roles and Responsibilities

The SOCS forum will get input from the Heads of IT Forum, the Oil & Gas Information Security Forum (OGISF), and steer the direction of the forum, led by the Chair, but by consensus of the group in a democratic manner. The Chair of the SOCS forum will also attend the Heads of IT Forum to represent the interests of the SOCS Forum in that group, and get direction/input from the Heads of IT.

The Chair and Vice Chair shall seek to ensure that:

Terms of Reference – OGUK Special Interest Group

- the SOCS Forum accomplishes its objectives by planning workgroup activities and evaluating implementation and progress of work;
- the SOCS Forum is made up of a cross section of industry and has a sufficient level of experience; and
- any product delivered by the SOCS Forum represents a balanced industry viewpoint.

The SOCS forum will refer to the Heads of IT Forum and/or OGUK's HSE Directorate for support, linkage within OGUK, and assessing all matters relating to government and public relations and media services.

Digital Work Groups

The SOCS Forum provides a platform for Task Finish Groups (Digital Work Groups) to be formed to own and work specific work streams, and for progress to be communicated. Task Finish Groups typically exist for a defined period of time to deliver a specific project.

Each Task Finish Group will generally be led by a member of the Forum & resourced by the Forum using the full range of resource available within their respective organisations. Each Task Finish Group will publish an activity plan highlighting where support from the Forum will likely be needed, and will provide regular updates for endorsement at Forum meetings.

Meeting Frequency

The full SOCS Forum will generally meet in the following format:

- as a combined body Skype Update Call: Weekly
- face to face meeting: 4 times per year
- specific challenge/sharing workshops: As required

Each meeting will have a written agenda which will be circulated in advance. Meeting minutes will be taken and circulated. Additional ad-hoc meetings may be convened with the approval of the Chair should there be a specific need to discuss or finalise any particular issue.

A senior Oil & Gas UK Manager will attend to facilitate meetings of the group, and to ensure that:

1. Oil & Gas UK's Competition Law policy is implemented, and that all meetings comply;
2. All meetings are minuted, actions tracked, and communication between members of this Forum and other relevant digital forums and groups is effective;
3. All documents arising from meetings are appropriately managed and shared.

External Linkages & Reporting

The SOCS Forum is led by industry. It will liaise with various bodies as required:

- to the Heads of IT Forum via the Chair at scheduled HOIT Forum meetings
- OGISF (Oil & Gas Information Security Forum) on a quarterly basis
- Through OGUK to its other digital SIGs and Forums

Terms of Reference – OGUK Special Interest Group

One important aspect of the Forum's work is to share information on active security incidents to allow other members of the group to take proactive measure to protect their own organisation and assist any other member of the group that has been affected by an incident.

Any information shared will be in compliance with Competition Law, in accordance with OGUK's Competition Law Policy. Information shared may be anonymised where appropriate, with clear conditions of use established according to standard operational cyber security information sharing practices (e.g. the Traffic Light Protocol[1]).

---

[1] See: https://www.us-cert.gov/tlp