Statement of Principles

Security of Seismic Operations

Revision Date: April 2014

Date first issued: 2003

This document includes the Statement of Principles, a description of the issues (with examples) and contractual language.

Key Words:

- **Area of Operations**
- **Client**
- **Consultant**
- **Contract**
- **Contractor**
- **Exploration Risk**
- **Force Majeure**
- **Seismic Operations**
- **Subcontractor**
- **Tender**
- **Third Party(ies)**

Terms that are in bold type are defined in the Glossary of Terms which forms part of this family of Statements of Principles.

IAGC
1225 North Loop West
Ste. 220
Houston, TX 77008 USA
P. +1 713 957 8080
iagc@iagc.org
www.iagc.org

Statement of Principles

The vision of both Client and Contractor

The vision of both **Client** ant **Contractor** for approaching security risks should:

1. Recognize the urgency, especially when personnel and equipment are at risk;
2. Be the one that is precautionary and which focuses on protection of personnel and equipment; and
3. Coordinate risk management through the value chain, including **Sub-Contractors.**

As there will rarely if ever be certainty about the exact level of the risk to an operation and the precise effect of changing conditions, a bias toward caution and conservative protective action should prevail in all security risk management decisions.

Security related risks (as described in the first section above) should be assessed in advance for the geophysical operation, its area and any other relevant areas (e.g. transfer and supply locations), and all security risks should be identified and described. This should be done by the **Client** and provided at the invitation to **Tender** stage. To ensure common understanding and to harmonize what may be different scales or terminology, levels of security risks (hereinafter referred to as Security Risk Levels) should be set out at **Tender**, and subsequently agreed upon between **Client** and **Contractor** before the project commences[1]. Each risk identified in the assessment should be

[1] For example, the parties might agree that four Security Risk Levels are reasonable, that they will mirror Client's risk management approach, that the lowest threat level will represent minimal risk and be called Level 1 (corresponding to **Contractor's** blue level), and the most elevated level will represent an imminent, severe risk and be called Level 4 (corresponding to **Contractor's** red level).

evaluated for each Security Risk Level, and control measures and strategies for managing each risk at each Security Risk Level should be developed and proposed by the **Client** at **Tender**, reviewed after **Contract** award by the successful **Contractor**, and be mutually agreed prior to commencement of project operations. The **Client** should also disclose its internal security risk assessment and analysis which defines what Security Risk Level is assigned for **Client** personnel who might subsequently work in the **Area of Operations**, and if discrepancies exist between the two, provide its rationale for the difference in standards.

In spite of proper security risk management, security incidents that may eventually impact geophysical operations cannot always be predicted at **Tender**. As such, the cost of security incidents and the implementation of any needed control measures, as well as all indirect costs should be considered costs associated with **Exploration Risks**, and all such costs should be the responsibility of the **Client**.

Costs which may be incurred during the life of a project due to security risk management, including those from changes in Security Risk Levels during the implementation of the project, can be both direct and indirect costs, and can include costs associated with the following (examples, not a complete list):

- Security resources such as watch guards, protection escorts, armed guards or military assistance, if required;
- **Contracted** security assessments and intelligence service and/or security **Consultant**, if required;
- Physical security measures such as fences, machinery needed to erect and level sand/dirt berms, razor wire barriers, additional perimeter lighting and associated generators etc.; hardening of vessels;
- Secure transportation to and from the **Area of Operations** if required.
- Changes in transportation routing, logistical support, etc. necessitated by changes in Security Risk Levels during the project;
- Possible regulatory changes regarding security;
- Additional personnel training necessitated by unusual security conditions;
- Damage to or loss of equipment, facilities, etc.;
- Reduced operational productivity due to:
    a. Equipment damage or loss;
    b. Limitations on access to work site;
    c. Imposition of needed control measures;
    d. Availability of personnel
    e. Loss of commercial or business opportunity

The Case of Piracy at Sea

Even if various areas exposed to piracy risk need specific risk assessments and thus specific controls; considering the vulnerability of seismic vessels to attacks (low speed, low free board and staying in the same location), we recommend drafting vessel security plans in conformance with the following lines for higher risk areas:

- Vessels security is based on deterrence;
- We do not consider early detection and escape a totally robust mean to prevent attacks;
- All vessels should be hardened and fitted with a citadel;
- Non-lethal weapons do not ensure efficient deterrence, thus lethal weapons might be recommended by risk assessment, and subject to approval by relevant authorities;
- Rules of engagement have to be clear with detailed steps (starting with radio and visual warnings up to warning shots), in line with international rules, and drilled; Masters overall authorities and chain of commands have to be clearly defined; best practices on stowing of weapons and ammunitions commands have to be clearly described;
- Security **Contractors** have to be assessed and screened according to best practices;
- Security resources supplied by local navy and / or vessel flag state are preferred;
- Security resources and means have to protect the whole seismic fleet, including small boat operations and logistic journeys;
- A relevant risk assessment has to be conducted before deciding to locate armed guards on the seismic vessel(s) or on dedicated security vessels, depending on the flag legislation, the company rules of the various stakeholders and the applicable local legislation if any;
- When seismic survey is taking place in **Client** oil fields with already existing security resources, these resources could be adjusted and allocated to seismic survey when feasible.

To accomplish the foregoing, the following points should be covered in all **Contracts**

1. Define security risk assessment criteria to set appropriate Security Risk Levels which in turn characterizes the required control measures for each level.
2. Recognize the assigned Security Risk Level as being dynamic and that it should be revised/ reviewed if and when events change the Security Risk Level at any time during the project.
3. Specify that **Client** will pay for direct and indirect costs incurred from **Tender** submission to project completion due to security risk management and possible changes in the Security Risk Level. It should be specified that indirect costs include reduced or suspended productivity, which should be covered at full production rates, as well as loss.
4. Provide for immediate notification and response when information or events necessitate a change in the Security Risk Level.

5. **Client** identify its point of contact (and all contact details) that has authority to approve a change in the Security Risk Level; that person must be immediately available 24/7 the entire time operations are in the field. If a decision from **Client** is not immediately forthcoming or

   Contractor cannot immediately reach the point of contact, **Contractor** is authorized to change the Security Risk Level as needed.

6. Assignment of responsibilities for requesting and providing military assistance when required.

7. If it is agreed at **Tender** or before commencement of operations that **Client** will implement or provide any of the control measures (e.g. mine clearance, on-call armed guard or protection services, evacuation transportation, etc.), then:

   a. Specific time requirements for their implementation should be clearly set out, and the rights and authority of **Contractor** if a control measure is not timely implemented; and

   b. **Contractor** should retain the right to verify the quality or adequacy of the service based on agreed standards and, if the results or the service do not meet the agreed standards, to reject (either results or the service provider) and secure its own alternative at **Client's** cost.

8. Termination clause if security measures cannot be implemented in a reasonable timeframe.

9. Establish who has the right to shut down operations due to security issues. This must be based on mutually agreed timelines prior to start of the project. If these timelines are not subsequently met, **Contractor**, having the overall authority and duty of care of its personnel, has the right to shut down operations without penalty.

Commercial Context

Seismic Operations often must be carried out in areas that may be exposed to security related risks of a criminal, civil, tribal, political and terrorist nature. These risks can be regional in nature or more location specific and can include mugging, theft, blackmail, extortion, threats, car hi-jacking, kidnapping or piracy. **Seismic Operations** are also exposed to location specific security risks such as unexploded ordnance, chemical, biological or radioactive contamination, as well as the unique risks associated with areas with disputed borders.

Security risks that develop into an incident can cause personnel injury and death, destruction or loss of equipment, and delays to operations. Poor management of the risks almost ensures these effects will increase. In addition, it must be recognized that operational security risks are dynamic in nature and can change over time. Thus strategies for preventing and mitigating security risks must be flexible and adaptive from **Tender** submission to project completion.

Every employer (both **Client** companies and **Contractors**) has a "duty of care" towards their employees: a responsibility to provide as safe an operating environment as is possible when taking into consideration location, risks, costs, etc. The E&P industry has generally adopted an approach for managing these risks that involves assessing the risks in advance and, based upon the assessment, developing management

strategies that will prevent an incident from occurring (or at least minimize its likelihood) and mitigate (reduce) the severity if an incident occurs. It also provides for real time monitoring of conditions and adjustment of prevention and mitigation measures as changes warrant.

To avoid any possible delay in undertaking or adjusting prevention and mitigation measures (from now on referred to as control measures), as well as to avoid subsequent contractual disputes which could result from a lack of clarity in these areas, contractual terms must clearly address the security risk management approach, as well as the responsibilities, timing and costs associated with the agreed approach. Additionally, the security risk assessment must determine necessary control measures that need to be implemented, both prior to project start up and if changes in control measures are needed based on escalation or de-escalation of security risks any time during the project.

E&P activities are present in numerous areas where security related risks are present. In particular terrorist activities in the Middle East and South America, civil unrest in African countries, piracy in Gulf of Guinea and Indian Ocean are of growing concern, and the oil industry and services related to the oil industry are a prime potential target.

Recent Examples

1. Following the award of a certain land seismic **Contract** the security situation changed dramatically. There were several attacks targeting foreigners, office buildings and a compound. Unclear contractual language regarding responsibilities and allocation of costs complicated the swift implementation of adequate security measures.

2. A **Client contracted** a seismic **Contractor** to operate in an area that, due to security threats, was classified by the **Client** as a prohibited area (i.e. an area in which the **Client** itself would not risk its own employees).

3. A **Client** was to provide mine clearance but sought to do so in a manner that did not meet the minimum quality criteria for mine clearance necessary for safe operations (as defined by the seismic **Contractor**). The quality criteria for mine clearance were not defined in the **Contract**, which led to a considerable delay in the project implementation.

4. Repeated theft of vehicles by armed bandits resulted in injury to personnel (particularly drivers) and damage to or loss of vehicles, necessitating increased security and increasing project costs.

5. Limited or nonexistent **Client** community relations resulted in aggressive clashes with local communities which impacted the implementation of a marine project.

6. A land seismic **Contract** was awarded for an area with known armed conflict between government and local factions. Despite a large, heavily armed force being assigned to protect the operation, it was attacked. Several members of the protective force were killed in their successful defense of the operation, and the operation was halted.

7. While conducting **Seismic Operations** around a **Client's** existing operations, several kidnapping incidents occurred involving **Contractor's** personnel, one of which included gunfire. Feeling it unsafe to continue, **Contractor** requested the appropriate **Force Majeure** / community disturbance **Contract** provisions be invoked and **Contractor** be allowed to remove

personnel and equipment from the area until security conditions adequately improved. The **Client** denied **Contractors** request.

8. An offshore service vessel had been attacked and hijacked at ten nautical miles from the coastline on its way to deliver equipment to an oil rig. The attack had been performed by pirates using five speedboats. Fortunately, the crew and vessel were released three days later.

#####

See other IAGC Statements of Principles for related topics (e.g. Interference by Local Populations, **Force Majeure**, Termination, **Third Party** Direct Action Groups, etc.).

For additional references, please see OGP's guidelines on security related matters (www.ogp.org.uk/) and Best Management Practices for Protection (BMP) against Somalia Based Piracy (UKMTO and MSCHOA – www.mschoa.org).