

Sep 29 2014

Irene Pietropaoli – The use of human rights indicators to monitor private security companies operations

Damiano de Felice

Private security companies (PSCs) often operate in areas of conflict or weak governance, in the absence of effective regulation and with a high risk of implication in serious human rights abuses. As a result, governments and industry representatives, sometimes with civil society's participation, have developed several guidelines and codes of conduct that seek PSCs commitment to human rights standards and monitor their activities.

Two key multi-stakeholder initiatives are the [International Code of Conduct for Private Security Service Providers](#) (ICoC), and the [Voluntary Principles on Security and Human Rights](#) (VPs). Such initiatives are not formally linked and target different audiences: the ICoC is aimed directly at PSCs, while the VPs at extractive companies contracting private security services. Other main instruments include guidelines and certification standards, such as: the series of ANSI standards on PSCs developed by ASIS International ([PSC.1](#), [PSC.2](#), [PSC.3](#) and [PSC.4](#)); the [Industry Stability Operations Association \(ISOA\) code of conduct](#) and the [Guidelines for Private Maritime Security Companies](#) (ISO/PAS 28007:2012) developed by the International Organization for Standardization (ISO) to provide guidelines for shipping companies deploying privately contracted security personnel.

Measuring Business & Human Rights is carrying out a study to clarify the possible intersection between such initiatives and highlight common issues, in particular through the analysis of the use of human rights indicators.

Despite their differences in process, structure, organisation and requirements, all these initiatives address the issue of security and human rights. While not formally connected, they are potentially mutually reinforcing. For example, the ICoC Association has identified PSC.1 and ISO/PAS 28007 as the first two standards necessary for assessing whether a member company's policies meet the requirements of the code. An external expert is comparing the ICoC and PSC.1 to establish whether certification to PSC.1 will be enough to grant certification to the ICoC or whether additional information related to the human rights impacts of the company's operations is required. ISO is also working at a new certifiable management standard for private security company operations ([ISO/PC 284](#)), whose human rights content is informed by the ICoC.

In order to assess company compliance with standards and codes, measurable criteria are required and some initiatives have developed specific human rights indicators. Such indicators, however, are not designed to measure the **human rights impacts** of the company, but to assess the member company's compliance to the set of principles or standards. For example, the VPs process has developed two documents that include human rights indicators: the [Key Performance Indicators](#) (KPIs) and the [Audit Protocol](#). Indicator 2 of the KPIs deals with the comprehensiveness of stakeholder consultations, necessary to have a clear understanding of the operating environment. Companies receive points for a total out of 100% for: number of consultations; range of actors consulted (communities, local media, authorities etc...); and whether they let independent parties facilitate the consultation. But none of these factors guarantee outcomes, or provide any indication of the human rights impact of the company's operations.

Another example is Indicator 5 of the KPI, concerning staff training. This indicator only check whether the different actors responsible for security have received training on human rights, but overlooks the quality of the training, possible outcomes and impacts. The Audit Protocol also includes a set of indicators to provide assurance that the systems and processes required by the VPs are in place and being complied with by the company. Such indicators are based on the KPIs and do not provide for weight of human rights impacts.

Likewise, measurable criteria under PSC.1 (management and governance; selection, screening and vetting of personnel and sub-contractors; training of personnel; procurement etc...) do not include any measurement of possible outcomes and human rights impact of the member company's operations.

The **lack of transparency** is a common problem, especially in relation to the reporting systems. Lack of transparency is evident in the VPs, due to the confidential nature of the dialogue and that public reporting remains voluntary. The KPIs recognise that companies may have their own protocol for recording incidents and may be unwilling to document in writing therequested information. They describe it as a "unique opportunity for the companies to hold themselves accountable first". Similarly, audit test results are confidential under the Audit Protocol. PSC.1 includes measurable criteria for managing, reporting and documenting incidents, as well as for the company grievance processes. These are also handled in confidence and do not include any information provided by affected parties. Similarly, complaints under the ISOA Code of Conduct are handled in confidence with only the complainant and the accused company appraised of progress. The ISOA justifies this high

level of confidentiality to facilitate the provision of information by companies. The ICoC reporting is also covered by the “necessary confidentiality and non-disclosure arrangements” that allow companies to submit to a governance and oversight mechanism and assess their performance.

The initiatives analysed have also a different degree of **multi-stakeholder consultation**. For example, the ICoC was developed through a transparent and inclusive multi-stakeholder process (with representatives from governments, industry and civil society) and overseen by an independent institution. All the information related to the ICoC process, the minutes of the three Working Groups, as well as the drafting of the articles establishing the oversight mechanism are publicly available. On the contrary, in the member-based associations, like ASIS, information is available only to members. Likewise, the VPs Audit Protocol was developed on by a group of corporate-only participants and the protocol itself is the only document publicly available. ISO also lacks a technical committee and a mix of stakeholders with necessary human rights expertise.

Third-party oversight, in relation to monitoring, auditing, certification, or accreditation, has a mixed degree of development in the different initiatives. The VPs lack third-party oversight as monitoring of, and compliance with, the principles is up to individual companies. Likewise, under the Audit Protocol, compliance is limited to the data provided by the company, consisting of its policies, procedures, guidelines and examples of country implementation, without a third-party data supplier. For instance, indicator B.4 and B.6 look at whether a company has a procedure for reporting and for addressing security-related human rights allegations. The company reports on its procedures or mechanisms alone. To verify compliance, the auditors are required to confirm that such procedures are in place. This is done mainly through discussions with the executive responsible for the VPs, without checking the company information against any other data.

The ICoC, on the other hand, formed the ICoC Association in 2013 to provide external and independent third-party oversight mechanism. The Association’s mandate is to ensure the effective implementation of the ICoC through certification, human-rights-oriented field monitoring, and a compliance procedure. Importantly, the Association is mandated to gather and receive information from the public on whether member companies are operating in compliance with the code. The ICoC also establishes an auditing process through which independent auditors conduct on-site audits, including in the field, and report the data gathered to the oversight mechanism. This will in turn verify whether the company is meeting the requirements and, if not, what remediation is required.

Compliance with ISO/PAS 28007:2012 can be assessed by first, second and third party certification. The new ISO/PC 284 will also be a certifiable standard, to which organisations can demonstrate their conformance through a third party certification audit. Likewise, conformance to PSC.1 standard is validated by an independent third-party accredited certification body – which must first be accredited by an independent accreditation body. Here there is the opportunity for external parties to provide feedback and report concerns at all levels of the certification process.

Related to the external oversight is the issue of **accountability and enforcement**. Enforcement is lacking in the VPs. These call for companies “where appropriate” to include the VPs in legally binding contracts with private security companies. Some extractive companies have done so, making adherence to the VPs a mandatory part of the agreement. But the company’s commitment to adhere to the VPs is voluntary, the actions under the VPs are not verified or enforced, and signatories face few consequences for failing to uphold the principles. There are no provisions for penalties in case of non-compliance, other than the possibility of being expelled from the VPs.

The enforcement of the ISOA Code of Conduct is guided by the publically available ISOA Enforcement Mechanism. This mechanism ensures that anyone can bring a complaint, based on the Code of Conduct, against an ISOA member company, for review by the ISOA Standards Committee. ISOA can expel members that refuse to address problems.

The ICoC is not a legally binding instrument, but some governments have already indicated that they will only hire PSCs that have signed the ICoC and agreed to submit to the accountability system. For example, the US Department of State said that ICoC Association membership will be a requirement in the bidding process for the successor contract to the Worldwide Protective Services programme. Similarly, conformance to the PSC.1 standard is required in US Defense Department contracts for private security functions, as well as those contracted through the UK Foreign and Commonwealth Office. This means that the interest of the company to comply with the human rights provisions goes beyond mere membership as non-compliance may affect its ability to procure contracts.

In conclusion, the credibility of these initiatives depends on their adoption of effective oversight and reliable complaints mechanisms that ensure remedy for victims, and a greater capacity to monitor compliance and to sanction non-compliance. The efficacy will also rely on PSCs acceptance of such independent external oversight, and on governments and other clients’ commitment to hiring only PSCs that are in full compliance. There is also a need for an open, transparent consultation process that includes extensive outreach to attract appropriate stakeholders and ensures that audits are conducted with the necessary human rights expertise. Assessing measurable criteria in relation to the human rights risk conducted as part of the certification process, needs to amount to more than a desk-based box-ticking exercise. Certification institutions, accreditations bodies and auditors need to gather information from the field and capture actual human rights impacts on the ground. While a certain degree of confidentiality is necessary in certain operating environments, the reporting process, especially when related to human rights incidents, needs to include public disclosure. This would help to ensure that certification goes beyond what the company chooses to report – for example on parts of the business where they have achieved compliance while ignoring areas in which they face human rights issues. A transparent and public report of lessons learned would be useful also to determine the compatibility between these initiatives. These steps may help to increase transparency and disclosure concerning the activities of PSCs, and to hold them accountable for human rights abuses.

Irene Pietropaoli



Irene Pietropaoli is one of the co-Directors of MB&HR and a PhD candidate at the Law school of Middlesex University, London. In the past years she worked as a researcher at the Business & Human Rights Resource Centre. She is now based in Yangon, Myanmar.

This entry was posted in [Human Rights Impact Assessments](#), [Management tools](#), [Reporting](#) and tagged [business](#), [human rights](#), [international code of conduct](#), [private security companies](#), [voluntary principles](#). Bookmark the [permalink](#).