Minutes, ICoC Working Group #1 Meeting: 24 June 2011 via teleconference

Attending :

- Mark DeWitt, Triple Canopy (USA)
- Ian Ralby, ADS Security in Complex Environments Group
- John Morrision, Institute for Human Rights and Business (UK)
- Andy Orsomond, Human Rights First (USA)
- Margaret Belof, UK Foreign Commonwealth Office
- Chris Mayer, U.S. Department of Defense
- Scott (for Doug Allison)

BEGIN 9:00 DC / 14:00 UK / 15:00 GENEVA

Sub-Group A (Assessment): Presentation of Findings

- General concept is that assessment and certification, under the ICoC, would build upon but not be limited to the standards
- ISO type standard can only be verified for business processes, and can't measure full measure of things required by the ICoC
- Deficiency at being able to evaluate the broader Human Rights impacts
- Once a company has achieved ISO certification, then it can apply for recognition by the Code of Conduct (after completing additional requirements—i.e. Ruggie Guiding Principles)
    - For ICoC recognition, additional measures will be required
- If the ICoC decides that it's going to issue a certificate of compliance and an "undesirable event" happens, it could pose serious legal issues
- If the board decides to certify companies, it could potentially be sued by any of the participants
- The decision to certify could provide a basis for suing
- Suggestion that ICoC registers a certification of compliance for the companies, rather than a certificate of approval
- If a PSC does everything right, there's still a chance of death or serious injury in these high risk situations
    - Fear of being sued may be somewhat overblown—there's not that many cases being brought against people when death occurs in complex environments
- We need to discuss the ability of being able to operate in parallel with ISO standards
    - A company issues a statement of intention to commit to ISO standards—that could go to ICoC as well
    - Can we get provincial recognition under the conduct at that point?

    - ISO external audit certifies business process, then phase 2 would be IGOM requirements
    - When you do your internal audit, then you would submit a report of that audit to the IGOM at that point
- Are we going to require everybody to get the ISO certification? If not ISO, then what?
    - Consensus seems that yes
- We need a recommendation as to whether ISO is the sole path, or a path to go that replaces something else
- The odds are that ANSI standards will be adopted rather quickly by ISO, but some states will allow their companies to just follow ANSI standards
- To say that we're going to require adherence to the ANSI standards may be problematic
- The ISO is allowing companies that are presently certified and recognized to perform audits every 2 years to comply with the recently changed laws (not many changes from 2010 standards)
- What are we actually certifying? We're not certifying that companies are compliant. We're certifying that they've gone through the steps of the code (like John Ruggie's framework)—process rather than outcome
- What extra external auditing do we want to do and what do we want to do under the process of verification?
- Ultimately, the governing board is going to have limited capacity to oversee the operations of all these PSCs—we have to use other tools rather than inherent organic tools to this IGOM as much as we can; efficiency and management of resources
- IGOM has to retain for itself a level of certainty; how can we guarantee the audit skills of someone from ISO?
    - These certifying bodies will have to be approved by the IGOM
    - Internal audit reports going to IGOM would increase transparency
    - Lines of communication and checkpoints between IGOM and ISO
- There has to be a human rights impact assessment tool of some sort
- ISO certification process: "corrective actions" stage report is a public report
- What about companies outside of the US and UK who want to be full participatory members of the ICoC but don't want to go through the ISO?
    - Is the IGOM going to have the ability to engage with a company that doesn't want to go through the ISO process?
    - Not in favor of giving alternative paths because it could lead to venue shopping—companies looking for the easiest path
- In effect, the ANSI standard process is developing something that will become a central and integral part of the code

- It would be a bad idea to try and do this all on our own because the expertise lies in the ISO certification process
- Maybe ISO will be the primary path, then the IGOM will look and see if other paths need to be available as well
- There's going to have to be a MSI discussion about what that ISO certification gets you, or what could be another avenue without creating a venue shopping opportunity
- Right now, in the US, you can require ISO certification *or* its demonstrated equivalent—but there is no demonstrated equivalent
    - We could do the same-if something else comes along, we can vote to use that
    - Lots of small companies are going to be asked to go through this big process that costs a lot of resources
    - If we say the ANSI standard or its demonstrated equivalent, then that would allow time for the ISO standard—Could say the ANSI standard or its equivalent (as approved by the IGOM)
- Desire to create something that is efficient and has a sustainable management—leveraging outside standards would be very helpful; IGOM just needs to be able to ultimately retain the authority to decide who meets the standards
- The next step will be to answer the Human Rights Impact Assessment
- When looking at levels of participation or recognition, what is the incentive to reach a higher level of certification?
- Being a signatory to the ICoC would mean that you've been approved by external audit IGOM measures and the Human Rights Impact Assessment
- Suggestion to maybe talk to an expert about how ISO works (Mark Siegal)

Sub-Group B (Transparency Reporting): Mark DeWitt

- Overall Reporting Structure
    - Reporting should be divided into 3 principle areas
    1. Informational Reporting—sig cos should provide an initial registration report with basic, relevant info
        - Should be publically available and regularly updated
    2. Bridge Report—used to monitor signatory company activity
        - Transparency
        - Looking at 3rd parties to provide comments
        - Customers should be able to verify status of company
    3. Sustainable Reporting
        - Recommendations for the SigCos—could be made publically available
        - Some of these could also be incorporated into the bridge reporting
        - A concern that serious incident reporting can often be misinformed

- Serious incident reporting would be good if it was a very basic, generic type of report
- The risk of a situation in which the IGOM representative has to answer questions from the outside world that he/she has no knowledge of
- Would it be better for the IGOM to not even be involved in all in that sort of questioning? More conservative approach to media inquiries—IGOM would say: If you have questions regarding the incident you should talk to the company
- But, the IGOM will be somewhere that the media goes to
- IGOM registration form should put "point of contact for media inquiries" so that IGOM can lead media somewhere else
- Having the IGOM aware of incidents so that they can begin the process of following up is important
- To preserve the credibility of this institution, the permanent secretariat needs to be made aware of incidents and then there will be some process of follow up
- Initial incident needs to be reported so that the follow up can begin as soon as possible
- Need to take a look at what kind of information needs to be reported
- Important to distinguish between what is likely to get public attention and should therefore be reported right away, and what can be made on a more routine basis
    - Where do you draw the line as to what kind of incident generates an immediate report and which kind of report goes into the periodic report?
- Worth looking at the difficulty of maintaining data in the EU—maybe we should talk to someone who has expertise in data protection internationally?
- Mark will follow up with data privacy & security expert
- Possibility of creating a black list for employees who have been discharged for serious code violations / other behavior indicating unfitness for working in security—certain implications to look at
    - If we do this, there'd have to be some kind of paper trail (probably with the IGOM)—this is an issue that will come up, even if we don't go as far as creating a black list
- Facts about certain incidents will have to be kept secret, while other parts will be open to the public
- Maybe one process for reporting (not 2 streams) just with separate annexes

Sub-Group C (Internal & External Oversight): Andy Orsmond

- 3 issues to address:
    - Lessons from other MSI about how to divide up what is done internally and what is done externally, where do you draw that line

    - Who do you end up giving external responsibilities to, what criteria do you use?
    - Is there a processing for crediting these groups? What kind of qualities are you looking for in these general areas
- Look at how this works from a holistic perspective
- Once we understand what the ISO process does, we'll have to layer on top of it—most likely this will be primarily external audits
- The ISO process can provide communication to the IGOM

- Round of 2nd discussions for sub groups: by July 1st
- July 8th would be the date for the next WG call
- Work toward a final product in accordance with the July 20th deadline
- Bruce de Gray is available on the 6th of July for a 2:00 call (UK time)

END 10:00 DC / 15:00 UK / 16:00 GENEVA