For more information, please contact:

**InterAction Security Unit**

John Schafer  
Director of Security  
j.schafer@interaction.org

Pete Murphy  
Associate Security Coordinator  
p.murphy@interaction.org

---

**Security Collaboration**

**Best Practices Guide**

*Transitioning from a culture of “need to know”, to one of “need to share”.*
Transition Indicators to an Intermediate or Full Spectrum Collaboration..........................................................26
Intermediate and Full Spectrum..................................................................................................................................27
InterAction Starts ANSO ........................................................................................................................................27
Conclusion ............................................................................................................................................................28
Acknowledgements ..............................................................................................................................................30
Addenda ...............................................................................................................................................................31
Annex 1 - Pakistan Security Collaboration (Informal) .........................................................................................31
Annex 2 – Haiti Security collaboration (informal) ...............................................................................................35
Annex 3 – SPAS (Full Spectrum – Weekly Report) ............................................................................................39
Annex 4 – Levels of Collaboration ........................................................................................................................44
InterAction Security Collaboration Self-Test ........................................................................................................45
Annex 5 – SLT Revision Report ..........................................................................................................................45
Figure 1: Security Information Flow Diagram
Introduction
Need for Sharing Security Information

In last decade the demand for sharing security information, and consensus in favor of such collaboration, has grown among the Humanitarian NGO and IO community. Attacks against aid workers have increased sharply since 2006, with a particular upswing in kidnapping.¹ As security risks and breaches increase in numbers, access to and management of security information evermore prefaces resolving a crisis and handling the fallout.

Today, the expanding humanitarian community and its scope of impact around the world are accompanied by new data mapping software, an influx of recordable information, and scholarly and experience based research. For the time being, despite some major strides in security management, aid organizations face serious dilemmas in certain threat environments, with short term adaptations often compromising long term security.² There is widespread agreement that to counter this increased risk to staff, greater NGO collaboration on security is required. Despite this, formal collaboration on security issues remains rare. Where mechanisms do exist, they tend to be ad hoc and reliant on personalities involved and, consequently, are rarely sustained.³ More recent evidence is suggestive of change, as some agency field offices are driving the development of operational guidance and protocols out of necessity and some headquarters are beginning to take up the issue for organization-wide policy development.⁴

Purpose of this Guide

¹ (HPG Policy Brief 34, April 2009) Providing Aid in Insecure Environments, 2009 Update, Abby Stoddard, Adele Hamer and Victoria DiDomenico

² (HPG Policy Brief 34, April 2009) Providing Aid in Insecure Environments, 2009 Update, Abby Stoddard, Adele Hamer and Victoria DiDomenico


Staff safety and security is an overarching aim for the humanitarian community. The authors’ goal is to provide a framework for practice of full spectrum (inter-agency and stake-holder) security collaboration. The purpose of this guide is to enhance security collaboration in the field by identifying relevant trends in security information flow, techniques of collection, management and dissemination of security information. Focus on security collaboration mechanisms and consistent exercise of their functions will provide security professionals and NGO-IO humanitarian stake-holders with the best means to the most desirable end – safety and security of their staff and mission. Even where NGOs recognize the need for a security collaboration mechanism, it can prove extremely difficult and slow to get a structure established and maintained, due to a lack of agency commitment and agreement, problems with funding, and availability of experienced staff.⁵

A security collaboration mechanism is designed to enhance sharing of relevant safety and security information. For this enhancement to take place the collective community or participants must identify and breakdown the barriers that block vertical and horizontal communication within and between stakeholders. The most expeditious means of accomplishing this goal is to establish security collaboration mechanisms for those operating in environments of elevated risk, or in complex emergencies.

In analyzing security collaboration mechanisms output [dissemination - or the products that are placed in the stake holders hands,] we map information flow processes and categorize them into either an informal, intermediate, or full-spectrum type of mechanism. We identify three levels of security collaboration and types of mechanisms in the field:

- Informal
- Intermediate
- Full spectrum

Levels of security collaboration vary from single-minded, isolated, unacknowledged efforts with unexpected results; to timely, coordinated, professional, experienced efforts with contingency structure.

Intended Use

“Everyone likes coordination; no one likes to be coordinated.”
~ Michael O’Neill

- Sharing security-training resources between the UN and NGOs is not part of the “standard operating procedures” of either. Sharing is often far from being collaborative or cooperative.
- Greater efforts are required on part of both the UN and NGOs to be more open about accessing and truly sharing training resources.
- Simple considerations, such as larger venues or more inclusive and diverse curricula, open up the possibility of increasing the number of individuals that are trained, as well as promoting a better understanding of the various approaches to security and how they impact on one another.

“Saving Lives Together: A Framework for improving Security Arrangements Among IGOs, NGOs, and UN in the Field”
November, 2006

It is impossible to properly provide an informative analysis of a security situation without collecting and managing of relevant information. Collection, management and dissemination of information must be monitored by a designated professional, or focal point, who is chiefly responsible for facilitating the process. Security focal points must provide the technical security inputs and advice that allows management officials to make informed decisions for managing security risks. Security risk management therefore requires good teamwork between those who plan and direct NGO operations and those who advise on the security measures which enable them. This individual is a mediator who registers all sources of information, stakeholders’ goals, and facilitates the crisis to a mutually acceptable outcome.

When stakeholders are confronted with a crisis they need to be prepared to implement the Security Risk Management (SRM) process. As they begin to collaborate, the quality and quantity of

6 Security Risk Management (SRM) NGO Approach, InterAction Security Unit
information is a high volume unregulated gridlock, thus, the designated focal point for security collaboration plays the role of a “traffic light” in the information management process.

Although each collaborative mechanism may have a diverse structure, we find that the services and products (or outputs) are often very similar. Defining the three types of security collaboration utilized by Non-Government Organizations (NGOs), International Organizations (IOs) and other stakeholders, this guide will provide the security professionals a useful reference, with a visual representation of three levels of security collaboration available to the stakeholders.

This guide should be used in tandem with:


When a stake holder is participating fully, the collaboration mechanism should provide a more focused image (analysis), effective training, and advice. The end-user will then have a greater ability to interpret and compare the analysis to their individual SRA in order to adjust activities and/or locations of their programs. Organizations participating in the collaborative effort should value the products provided as equally as they value vertical and horizontal sharing of information. When a stakeholder in a region desires broader analysis, then a focal point can be attached to the network, thereby enhancing the overall image of the security situation.

---

Security collaboration exists when two or more agencies are willing to act together to address a mutually identified security concern, in the belief that this will improve security information and support for their staff and, as a result, allow them to deliver assistance to beneficiaries more effectively.

Terms like ‘coordination’ and ‘collaboration’ have been used in a wide range of security initiatives in different contexts. While it is important not to labor over these definitions, it should be recognized that ‘coordination’ is often a controversial concept in the humanitarian sector; some NGOs resist coordination for fear of being ‘controlled’ or swamped by bureaucracy and restrictions. Recently there has been a shift in favor of a ‘collaborative’ approach to security in the field.


---
Frameworks of Security Collaboration
Directions of Security Information Flow

Vertical communication travels up and down within stakeholder organization structure. Vertical information flow has two directions: ascending and descending. An example of ascending vertical information would be if an NGO field staff shares information with a supervisor, or if national driver shares information with NGO staff, or when headquarters shares information for analysis and research with a university or a think-tank. When a stakeholder in region collects its incident reports and sends them to headquarters for more detailed analysis, it is also in an ascending information flow. As information is analyzed and conclusions are drawn, it may then be disseminated in a descending direction to field staff. Descending information is more common, reliable and less biased due to its hierarchical top-down dissemination. Ascending information flow can be underdeveloped in most organizations due to fear of repercussion, organizational hierarchy, and saving face.

Horizontal communication is defined as information that is shared laterally between organizations and stakeholders. For example, horizontal communication occurs when ‘NGO A’ shares a security report with a forum or another NGO at the field level. Another example of horizontal communication would be when Security Director from ‘NGO A’ shares information with Security Director of ‘NGO B’ or a security consortium such as European International Security Forum (EISF) or the InterAction Security Advisory Group (SAG).

Another example of horizontal communication: when information is shared from the United Nations Department of Safety and Security (UNDSS) to NGO security consortiums via “Saving Lives together”. (http://www.undg.org/docs/9338/8_Saving-lives-together.pdf)

An argument could be made that an additional plane of communication – diagonal in nature – exists within security information flow. For instance, if an NGO in the field were to observe a security incident and report it directly to a consortium, like the InterAction Security Unit or EISF, bypassing other stakeholders, then the communication would be diagonal in nature. Another example of diagonal information flow is a visit, email or telephone call from local individuals to headquarters, to warn or make suggestions with safety and security issues in mind. Consortiums have had experiences in the past where an NGO vehicle was observed being car-jacked. Those observing the incident did not have any means to contact the field office to relay the information. The NGO called the consortium (diagonal communication) who then relayed the message horizontally to the security director of the NGO, who in turn relayed the message vertically (descending) to the county office in the field.
Hierarchy of horizontal and vertical communication should be framed by the Information Security Policy of the Organization (ISPO). ISPO should act as a guide for determining what information should be shared and who it may be shared with. It is important to note that a security collaboration mechanism should have ISPO that can assist in protecting identities of the victims and stakeholders as needed. The ethics of using privileged information in zones of conflict while managing security crisis are complicated. We have mentioned earlier that safety and security of staff and mission are overarching concerns for many NGOs. That translates the grey area of security information sharing to a more clear a goal of “safety first”. A security focal point must be able to filter specific information for purposes of ethical adherence, while effectively disseminating relevant information to further safety and security of staff and the mission.

The intermediate and full spectrum security collaborations should have an information security policy that filters potentially harmful information and builds trust among the stakeholders.

A policy of security collaboration will aid with breaking some of the barriers to collaboration by building relationships with other stakeholders.

When security incidents are not collected, managed and disseminated horizontally, the threat image of a region is difficult to ascertain.

Optimal application of stakeholders utilizing the horizontal and vertical planes of communication is demonstrated when:

- a Security Director from ‘NGO A’ consolidates information received in a situation report from the field (ascending vertical),
- and then shares the situation report with ‘NGO B’ Security Director (horizontal),
- who in turn relays that same report to his team in the field (descending vertical).
- The communication loop is then closed when the two teams in the field discuss the report (horizontal)
- and share the feedback with their respective Security Directors (ascending vertical).

Security collaboration mechanisms thrive when both vertical and horizontal communication continually ‘close the loop’ (provide feedback) and when stakeholders work in a coordinated fashion. This has been demonstrated successfully by ANSO in Afghanistan, and SPAS in Somalia, both which are operating as full-spectrum collaboration mechanisms.

**Barriers to Collaboration**

Sharing security information, incident and situation reporting, and surveying vulnerabilities does not come naturally. Security professionals, country directors, managers, both international and national staff have to be trained and practiced in safety and security. Security professionals often have prior training that focuses their minds on what would be called “need to know” information and/or various
levels of classification. In short this means that an incident that happens to a specific stakeholder would stay within the organization and it would not be shared horizontally to another stakeholder operating in the same region. The instances that the information would be shared would often be dependant on a previously established informal relationship. For example: if NGO A experienced an attempted carjacking, the report of the incident would only be shared vertically with the country director. If the information was shared horizontally it would be in the form of a verbal brief and shared only with those who were considered close friends, or “in the loop”.

Country Directors are very similar to security professionals except that the vertical information that they would share about an incident to the Regional or Headquarters offices is often not shared for a variety of reasons. Managers and international staff may not share information vertically to their own security professional or Country Director for fear of administrative backlash, admission of breaking a policy, or to save face. The national staff members who are on the frontlines suffer the brunt of NGO deaths and injuries. They often find themselves in a catch 22, feeling if they were to report an incident they may lose their job.

The preceding list of potential barriers to security information sharing is not exhaustive. Stakeholder organizational structure, mission, culture, tribal, regional, religious, historic, and ethnic misconceptions may obstruct collaboration and sharing of relevant security information. Some organizations perceive security as a hindrance to operations; others might place too much emphasis on their autonomy, not associating or collaborating with other stakeholders in the region. Some organizations view their mission as of the utmost importance, operating with no sense of community, that organization will not have minimal trust built up with the other stakeholders and will be operating in a vacuum with very limited safety and security collaboration. Security for one is security for all. Just one non-collaborating, self-centered stakeholder, may jeopardize safety and security for all.

For instance; a stakeholder may not relay important incident information that is indicative of a higher level of risk, other stakeholders may be affected by a high impact or even terminal event, rather than a near miss, or avoidance of a negative impact altogether.

Once barriers to sharing information are identified, collaborators must rely on their professionalism and values to find common ground and work towards a mutually acceptable solution.
Collaboration in the Field

The Three Types of Security Collaboration

There are three types of security collaboration mechanisms in the NGO world – Informal, Intermediate and Full Spectrum which organizations contribute to, receive information from, and participate in. These three security collaboration structures provide a more coordinated approach to security than that of each organization working independently. The collaborative effort relies on the principle that the actions of every stakeholder in a community affect the entire community. This approach also utilizes an underlying utopian theme that says “True security only exists when it is for the entire community.”

Security collaboration rests on three pillars; Collection, Management, and Dissemination of security information. When coordinated efficiently, security collaboration produces horizontal and vertical communication structures which add to the value and security of organizations operating with a sense of community.

Many NGO collaboration mechanisms exist and each is unique (ANSO, GANSO, Darfur, BINGO, SPAS, CCO). We can evaluate and categorize the mechanisms by the quality of output of each and the common elements that they share.

For the purposes of this document, collaboration will be assessed in categories based solely on output or information disseminated. The three types will be defined as Informal, Intermediate, and Full-Spectrum.

Informal Field Security Collaboration

Informal security collaboration includes dissemination or output that is basic in nature, such as an incident report, an SMS text, alerts or flashes that are most often verbal, open source news reports and sharing of rumors. Information that is shared between stakeholders rarely has any vertical input from HQs. At the informal level, the output does not contain any written analysis, plotting of security incidents, standardized formats, source reliability, or seasonal reports. The above examples represent trends and requirements of a formalized network of communication. A rotating chairmanship is generally associated with an informal coordinating mechanism. The chair rarely has the same experience and/or training as a full-time security coordinator and the funding for their position is often deficient or nonexistent.

Combined with high turnover rates, the historical and contextual points of view tend to be shallow. Often due to the part-time nature of the rotation, the chair is over-burdened with the running of their own programming, while also trying to balance the security collaboration needs of the community. The output provided varies from nothing at all to phone calls, conversations, text and email of warden messages, meeting notes, and other information gathered.
**Intermediate Field Security Collaboration**

Characteristics of Intermediate Collaboration include: rudimentary trend analysis, basic plotting of incidents, open source collection, dissemination of security incidents, and other reporting as needed. Often there is a state of flux between informal and intermediate collaboration. Without the provision of dedicated individuals to actively take charge of the collection, management and dissemination process, the transformation to intermediate collaboration can be painstakingly delayed. Often stakeholders struggle to create a perfect solution that is impossible to achieve. It is not until the funding of a full time effort has been secured that we see intermediate collaboration products being produced.

Without ongoing compilation of security data, it is difficult for the collaboration mechanism to be considered full spectrum. Full Spectrum assumes that sufficient effort has been invested and that some sort of trend analysis has been ongoing long enough to output seasonal or yearly trends.

Another characteristic of Intermediate Collaboration is that a majority of the security professionals employed by International Non-Government Organizations (INGOs) would be national Security Focal Points, however ultimate responsibility for safety and security lies with the Country Directors. They have the decision making authority, and yet they are wearing many different hats and usually cannot devote full attention to security issues, leaving many gaps in training and analysis. Additionally, when provided, the security training for country directors, often only amounts to a one day workshop.

**Full Spectrum Field Security Collaboration**

Full Spectrum Collaboration is characterized by data gathered, analyzed and interpreted over a span of time. Monthly, quarterly, seasonal and annual reports are disseminated, providing a sharper threat image which is commonly broken down by regions. Examples of Full Spectrum Collaboration include: the latest version of ANSO in Afghanistan, SPAS in Somalia, and the UN Security Information and Operations Center. Full-Spectrum Collaboration is more often practiced in regions with the greatest levels of risk. In places like Afghanistan, Pakistan, Sudan and Somalia, Safety and Security policy is adhered to rigorously and it is more common to see the humanitarian community work collaboratively to maximize resources.

The greatest difficulty concerning Full Spectrum Collaboration implementation is that it requires greater transparency and participation of the host nation. In Pakistan, Sudan and Gaza, efforts of NGO collaboration were hampered by government objections. Many international disaster and relief NGOs fostering and participating in the security collaboration process were exposed to government retaliation, interrogation, and sometimes physical abuse and expulsion from the country.

The implementation of new NGO security collaboration often meets resistance from national authorities, and NGO security officers become dis-invited to operate in countries such as in Sudan. For insecure and delegitimized national authorities, the word ‘security’ might translate as ‘intelligence operations’ resulting in frustration, and the sometimes limitation of the organizational mission and mandate. The word ‘safety’ may be chosen as an alternative, suggesting safety of the NGO staff, rather than intelligence gathering for international authorities. There are fewer barriers to the UN
involvement because it falls under the status of forces agreement. In Darfur, this situation has been resolved through the intervention of the UNDSS which assumed sole responsibility for the funding, staffing, and operation of a Full Spectrum Collaboration mechanism. Implementing partners perform up to ninety percent of the UN operations in areas of Darfur.

Looking closely at the examples above, we can predict that insecurity in Afghanistan in 2010 will continue to deteriorate. The data can be used in many ways by organizations that choose to mitigate the increasing risk trends; via programmed vacations during predictable times of insecurity (such as elections); or to increase budgets to enhance protection; or by avoiding or stockpiling in the most dangerous regions, thereby reducing the likelihood of incidents.
Verification Methods

Source Reliability Matrix (The Cycle)

A critical element contributing a full-spectrum Security Collaboration mechanism is the application of the Reliability and Validity Matrix (above) to the information provided to collaborative body's end users members. For instance, an "A" rating might mean a trusted source, such as vetted organizations contributing information in order to participate fully in the collaboration operation. That source may be considered completely reliable. An A1 (one) rating would indicate that the information was verified by a second - independent source. Most reports are somewhere in the middle; a "B-2", for example, is taken seriously. Sometimes, it is impossible to rate the reliability of source, most commonly from lack of experience with the individual reporting an incident, so an F-3 rating could be assigned to a report from an unknown source. An extremely trusted source might submit a report that cannot be confirmed or denied, so it would receive an "A- 6" rating.

<table>
<thead>
<tr>
<th>Source Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A:</strong> Knowledgeable with direct access to information</td>
</tr>
<tr>
<td><strong>B:</strong> Knowledgeable but no direct access to information</td>
</tr>
<tr>
<td><strong>C:</strong> Usually reliable</td>
</tr>
<tr>
<td><strong>D:</strong> Source is not usually reliable</td>
</tr>
<tr>
<td><strong>E:</strong> Source is not reliable</td>
</tr>
<tr>
<td><strong>F:</strong> We do not know</td>
</tr>
<tr>
<td><strong>O:</strong> Open source</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Validity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1:</strong> Suggested by several independent sources</td>
</tr>
<tr>
<td><strong>2:</strong> Very likely</td>
</tr>
<tr>
<td><strong>3:</strong> Likely</td>
</tr>
<tr>
<td><strong>4:</strong> Not likely</td>
</tr>
<tr>
<td><strong>5:</strong> Probably wrong information</td>
</tr>
<tr>
<td><strong>6:</strong> We do not know</td>
</tr>
<tr>
<td><strong>NFDK:</strong> No further details known</td>
</tr>
<tr>
<td><strong>GNK:</strong> Grid not known; location is not marked on available maps</td>
</tr>
</tbody>
</table>

FLASH = Current activity  ALERT = Possible future events

Using this model, a security incident may be reported to the Safety and Security Collaboration Mechanism by an NGO that observes an incident that occurred to another NGO and then shared with the coordinating mechanism (shown as the arrow below the Red Incident Box). Because the reporting NGO has provided reliable information previously and it has observed the incident, it may be reported (Disseminated) in a SitRep (Situation Report) symbolized by the arrow left of the yellow box; with ‘B - 2’ rating. Later the incident information might be confirmed and amended by another NGO, thus updated the incident as an ‘A -1’ rating. This is an example of how to fuse two systems (Collection Management Dissemination Process (CMD) and Source Reliability Matrix).
Information Validity

In reports disseminated by the safety and security collaboration mechanism, a source’s validity can be rated and accounted for. The rating is a composite reflecting experience with the source’s historical reporting, the source’s direct knowledge of what is being reported, and the source’s understanding of the subject.

Separately from the source evaluation is the evaluation of substance in the report: the information validity factor is plausibility, indicating that the information is suggested by multiple sources, not confirmed but suggested by a (single source), probably true, not likely, probably wrong, unconfirmed, and no further details known. (See Source Reliability Matrix)

Verifying Reliability of Information

When it is difficult to evaluate a report, confirmation may be a responsibility of those reporting the incident, the analysts, and/or those reporting or collecting the information. In a larger and more complex stakeholder community, this can be a difficult issue. In Afghanistan for instance, ANSO developed many relationships with the IOs, NGOs, the UN, and other actors, and over time has proven not to reveal its sources. Sensitive information is filtered before it is shared so it does not jeopardize the organization and individuals that supply it. ANSO also has been in the position to calm inflamed situations in order to protect an organization from rumors and/or actual incidents that need not to be reported while lives may still be in jeopardy. In a cooperative or smaller community of stakeholders, processes can be less formal, speedy and efficient.
Collection, Management and Dissemination

The Security Collaboration mechanism rests on three pillars: Collection, Management and Dissemination of relevant security information.

**Collection**

Collection activities include the following categories: post incident debriefings; liaison with other stakeholders; security reports and shared incident reports; past and current mission analysis; formal and informal communications; open source mediums; and other sources with stakeholders. The gathering of safety information for NGOs is usually conducted by security focal points. Collection activities vary depending on the source of information. Once the types of information have been collected and prepared, the ensuing report has the potential to be shared horizontally with other stakeholders. This is often the initiating of the CMD Process.

**Management of Information**

Once the information has been collected, a single point of contact compiles, categorizes, plots and analyzes the data. The data includes information about the local civilian population including its political, ethnic, religious, cultural, tribal, economic, and other social components and how those factors relate to the security of humanitarian/NGO operations. It carefully examines the various stakeholders, security incidents, trends, and unique programming vulnerabilities. Additionally, the data can often provide predictive security analysis, assisting humanitarian organizations in obtaining future mitigation funding.

In addition to the above, the management pillar:

- Closely examines the current and potential threat to identify factors pertaining to the blend of acceptance, protection, deterrence and avoidance strategies. The management process produces security risk analysis, training and other materials that are disseminated to the end users.
- Develops geographic information systems, social mapping, social networks data bases, and matrices, as required, to support the safety and security of humanitarian operations. These overlays may represent a wide variety of security issues, including mine information, host government infrastructure (for example, electrical power grid), population density, ethnic, religious, or tribal affiliation.
- Provides its products to stakeholders, including other management structures.
**Dissemination**

Once information has been collected the dissemination process begins. Mechanisms operating at the Informal Level of security collaboration often share information horizontally with other organizations in its raw form with little or no management of the information; individual organizations often send the information vertically to their regional officials or headquarters. Analysis of the information is then done at a regional and headquarters level, not at the actual location where the information was collected. The product (dissemination) provided to stakeholders is rarely formatted and is often transmitted through verbal conversations, emails, or round table meetings with other stakeholders.

Dissemination provided in the Intermediate or Full Spectrum mechanisms utilize formal notes, graphs that identify trends, maps displaying areas of insecurity, and other security related products. The management of the information is normally conducted in the same area that the mechanism is located. The materials produced are sent horizontally to other stakeholders and then the stakeholders send the synthesized product vertically to their regional and headquartered offices.

**Where it all begins (The Report)**

The most important and most critical element of the CMD process occurs soon after the incident. It is the actual report (record) that is filled out, specifying the particulars of the incident. (Example below)

With as much detail as possible and in a written format, each incident needs to be recorded in a manner similar to the example on the right. This includes the type of incident, description, impact, victim, location, effect on programming, and the regular date, time, etc.
The most important and most critical element of the CMD process occurs soon after the incident. It is the actual report (record) that is filled out, specifying the particulars of the incident. With as much detail as possible and in a written format, each incident needs to be recorded in a manner similar to the example on the right. This includes the type of incident, description, impact, victim, location, effect on programming, and the regular date, time, etc.

Although an initial verbal report may suffice, the written report has many internal and external functions, and serves as the basis for Information Collaboration.
**Internal Uses**

NGOs need to maintain the data on security related incidents in order to assist them in managing the risk associated with the exposures that they incur. Such reports enable them to follow up on any HQ support in counseling. Additionally, they may need the report for insurance purposes, internal tracking, country briefing, and even for training purposes.

**External Uses**

A sanitized version of the report can be shared with the community in order to provide better contextualized analysis, incident plotting, trend analysis, and in the mitigation stage — advice. Often a coordinator in the specific location can be used as a mediator with a local authority to raise issues that may be particular to an incident that occurred to an NGO without singling out the NGO involved. Finally, safety information, if disseminated among other stakeholders in the field, can help save lives and protect the organizational mission of the NGOs.

**Incidents**

The arrow on the right of the Red Incident Box represents the security incidents that are not reported. Stakeholders who reported incidents are represented by black arrows that descend from the incident box, thus initiating the flow of information.

**Stakeholders**

An incident that occurs to a stakeholder is often reported to the local office in the area of operations. Sometimes other stakeholders observe the same incident and it enters into the CDM process through other means. For example, an attempted carjacking of one NGO may be observed and reported by another, resulting in the incident entering into the collaboration mechanism. It may be observed (or verbally disclosed) by one stakeholder and then shared in a meeting or via text and email. In the Informal Collaboration context, there are times when there is not a standardized format and the report is given verbally, emailed, or texted.

There are arrows that are horizontally displayed in-between the stakeholders which represent information that is shared at the field and country office level. For example, the arrows symbolize a security focal point of an NGO providing the UNDSS with details of the incident. The UNDSS would then be able to include that information within its own system of CMD process thereby assisting the UN in developing a more focused threat image.
The United Nations Department of Safety and Security (UNDSS) (Dissected)

The UNDSS approach to security management is often seen in the Collaboration Model, and as a responsible stakeholder in many areas, the UN frequently has a Full Spectrum Mechanism in place. Incidents involving NGOs are included by the Field Coordinating Security Officer (FSCO) in the collection process in order to gain a more focused and accurate threat image. Through “Saving Lives Together”, FSCOs assist NGOs with briefings, advice and other services when feasible, and on a cost recovery basis when requested.

The ‘Saving Lives Together’ (SLT) initiative has been a significant move forward in collaboration between NGOs and the UN. SLT assists in fostering a sense of mutually supportive community (in theory).

There are many locations that also have other stakeholders that have applied Full Spectrum Collaboration Models. Third country interests, commercial entities (extraction industries), and development organizations are often other stakeholders that will have a Full Spectrum Information Collaboration, however there is not any formal agreement assists in the sharing of information.

Finally, foreign governments and security forces often are unwilling to share anything with stakeholders at all. The irony of this model is that foreign governments that have the resources, assets, and access to much of the information in the management process sometimes classify the information and do not share it with the organizations which they fund or host. One remedy to this problem is that a separate risk assessment should always be maintained as an unclassified document when it pertains to the safety of humanitarians operating in a specific theatre.
Field Reporting

Incident Plotting

Incident plotting as the name implies is simply recording incident locations (geo-referencing) so that they can be plotted on a map. The specific requirements for plotting incidents on a map will vary depending on theater of operation so specific details will not be covered in this document.

In general terms determining the location of an incident (not well defined at this point) can be accomplished through a variety of methods including GPS, digitizing from a digital map, map resection, or address matching. Regardless of the specific method used it is important that the following items be widely agreed on by all actors that intend to contribute geo-referenced incident data to the security effort.

Geographic Coordinate Systems

A geographic coordinate system enables every location on the Earth to be specified. There are many different coordinate systems, based on a variety of geodetic datums, units, projections, and reference systems in use today. Generally its best to choose only one organization-wide coordinate system for reporting and plotting. It is possible to use more than one coordinate system, however this requires that each set of coordinates also be accompanied by data indicating coordinate system used, datum, units and projection.
**From Paper to Digital Map**

In order to plot an incident location on a digital map most modern Geographic Information Systems (GIS) require that all coordinates be converted to latitude and longitude using decimal degrees. Storing coordinate data in this format allows GIS software to project coordinates to any other coordinate system required. The importance of the transition from analog (paper) to digital (GIS) cannot be understated.

Once coordinates are converted to the correct digital format, the number and type of analysis options increase to include virtually all database operations (query, sorting, grouping) and GIS operations (spatial analysis, data integration, map production).

**Anomalies**

Detailed to the right is the model currently used in Darfur. Restrictions by the government of Sudan prohibit NGOs from utilizing the Intermediate or Full Spectrum Models. NGOs initiated one attempt to assist the community in managing the risks they face by starting their own collaboration in 2006. However the Sudanese Government intervened by stating
NGO involvement was not appropriate. In 2008, the UN, ECHO, InterAction, and USAID initiated a modified Information Collaboration Model based on SLT. With the permission of the Sudanese Government and operating under a Status of Forces Agreement, the UN placed a model in Darfur to assist the NGOs. UN DSS and FSCO personnel were stationed in Darfur to work solely with NGOs to enhance their Risk Management Operations. Briefings, advice, communications, and training could be utilized by the NGOs. The NGOs agreed to place a Security Management Team together in each Darfur location to guide the FSCO in serving the needs of the NGOs.

The collection portion of the Coordinating Model is still handled by NGOs and they report the incidents to the designated FSCO who then utilizes the other assets of the UNDSS and provides further management and dissemination, thus completing a Full Spectrum Collaboration Mechanism. The individual NGOs still have the internal responsibility of maintaining the vertical communications within their organization while applying appropriate guidance and policy on how to share information horizontally to the UNDSS for further detailed analysis. The sooner that a problem or incident is analyzed, the greater the likelihood of report relevance and accuracy there will be.

**Disaster/Evolving Circumstances**

Lessons learned from the Lebanon 2006 crisis and from the Georgia 2008 crisis indicated that when conflict or disaster occurs in a region where development programs are ongoing, it is vital to implement a security collaboration mechanism as close to the triggering event as possible. The InterAction Security Unit has found that NGOs that are already engaged in development and humanitarian assistance are often overburdened by the emergency response because staff members often tasked with additional responsibilities become overburdened and the security and safety issues are not prioritized.

When the UN becomes engaged the local UNDSS will be overburdened by SLT requests from individual NGOs. A single collaborative security office can assist in managing the information and service requests. The collaborative security approach is essential in a sudden onset disaster or evolving hostile environment. The collaborative mechanism can provide Flashes, Alerts, Sitreps and other products to the members that would clearly articulate the evolving risks. Additionally it would host meetings, provide assistance and act as an advocate.
Consortium Collaboration Mechanisms

The European Initiative Security Forum (EISF), InterAction SAG, and ICVA (among others) comprise a collective of NGOs from their respective country or regions.

Recognized by the UN, they deal directly with the UNDSS NGO Liaison Office in order to coordinate security efforts, information, training and other activities. If the UN NGO Liaison dealt with each NGO directly, the unit would be bogged down by the hundreds of emails and phone calls from individual NGOs alone. Instead the Liaison Office deals with the Security focal points of the consortiums in order to best facilitate the SLT program. The consortiums have the CMD capabilities and provide Flashes, Alerts, Sitreps and other products to the members. They also conduct meetings, provide assistance, and act as advocates. Already mentioned is that they serve as the NGO representative to the UNDSS Liaison office.

Transition to Intermediate and Full Spectrum Mechanism

Often, when the UNDSS does not attend or participate in Informal security collaboration forums, the level of information drastically declines. It also has been noted that as the security situation steadily deteriorates that the ‘frog in the pot’ syndrome increases. Risk assessments that have been completed sixty days earlier can easily be out of date in a dynamic security environment. Smaller NGO’s often do not have the funds or skills required to operate in a deteriorating security situation and assistance from a collaboration mechanism may not be as important to the larger NGOs as it is to the smaller NGOs; but incidents affecting a small NGO almost always affect the larger. The security collaboration needs of the entire community could be better served with a stand-alone dedicated resource in keeping all the participating stakeholders on the same page.

When there is a complex emergency developing, uncertainty and indecision may lead some NGOs to resist the effort altogether. This uncertainty provokes lengthy debates about appropriate donors, hosts, and structuring that can dangerously delay the Intermediate Mechanism ramp-up. Furthermore as insecurity increases, UNDSS participation in informal mechanisms may drop off, as they are dealing with their own internal issues. This reduces their capacity to serve as a source of information to NGOs.

When discussions are beginning about the formation of an Intermediate Security Collaboration Mechanism, a few small but important steps can assist in preventing a decision process from stalling. It is important for each security director or focal point at headquarters, as well as those in field locations, to begin to advocate inside their respective organizations on the importance and benefits of a collaboration mechanism. Second, an assessment mission to the area looking at strengths, weaknesses, opportunities and threats should be dispatched; subsequent to which recommended
courses of action will be proffered. Once the assessment has been concluded, further advocacy should be pursued to develop ‘buy in’ from the community. If dissenting opinions remain they should be assessed to see if they are based on fact or opinion, the security philosophy of individuals, corporate culture, or personality conflict. If the dissenting opinions are in the minority they should not delay, hinder, or prevent the rest of the community from developing the Intermediate Mechanism that is identified by the assessment. Security professionalism can overcome personality conflicts. Focus on security needs of the community as a whole should outweigh minority opinions and the dissenters can always choose not to participate. The indicators below are provided to assist in identifying when a community may begin the process to transition from an informal to Intermediate collaboration.

*Trends and rapid onset insecurity and/or uncertainty is never followed by happy days.*

**Transition Indicators to an Intermediate or Full Spectrum Collaboration**

Indicators that suggest that while a location may appear calm the level of risk is increasing:

- The possibility of a complex emergency in increasing
- UNDSS (SLT) becomes overburdened with NGO requests
- Security incidents are increasing for NGOs and more analysis is needed
- Direct targeting of stakeholders takes place
- Significant increase of stakeholder presence in a short period of time
- Spike in incidents
- Natural Disaster occurs
- Political unrest
- Consortium security activity increases re: region

When the indicators are favorable for a transition from the Informal to Intermediate Collaboration Mechanism, the process of moving to the next level, or getting the dedicated resource to provide the services needed to the community, can be a risk to the community in itself. The decision process should not be left exclusively to either those on the ground or those at the Headquarters level. Security experts from both ends of the spectrum, combined with advice from those whom have experience setting up and operating previous successfully Intermediate and/or Full-Spectrum Mechanisms, should simultaneously be identifying funding options (ECHO’s NGO Security Collaboration Guide, 2006,) and the services to be provided, as determined by the stakeholder-needs assessment. This should prevent delay and the natural tendency to reinvent the wheel.
Intermediate and Full Spectrum

Although the matrix looks like a progression from one level to the next, that is not necessarily the case. When ANSO began it immediately was providing services at the Intermediate level. SPAS the mechanism in Somalia was able to provide services at the Full Spectrum at the onset. The key difference between Intermediate and Full Spectrum mainly lies in seasonal and time related analytical products. Without a single entity collecting a database of security incidents it is difficult for a mechanism to immediately provide statistical analysis of insecurity over time (trend analysis). A contextual analysis may be able to provide a general overview of trends and this could initially provide the output requirement of a Full Spectrum mechanism. As incidents and other information are continually collected, the disseminated analytical products should strengthen over time.

InterAction Starts ANSO

In the spring of 2002, Security Directors and Focal Points of several InterAction member organizations operating in Afghanistan combined resources to send a consultant to evaluate feasibility of dedicating a resource to collect, manage and disseminate safety and security information in that high risk environment. The consultant was to encourage the NGOs to work in a coordinated fashion in order to reduce costs and access resources of other stakeholders. This headquarters driven effort, modeled after the mid-nineties Guinea collaboration effort, is what is called ANSO today. The time period from concept to operational functionality was three months.
Conclusion

Inter-agency security cooperation can provide organizations with extra capacity at relatively low cost. Despite general praise and appreciation for security cooperation platforms such as those in Somalia and Afghanistan, however there remain very few others in existence.\(^7\)

Notwithstanding the gravity of the current climate of insecurity for aid work, humanitarian actors can be encouraged by the evidence of past years that serious investments in building security management skills and organizational capacity have apparently paid off as indicated by the declining numbers of major casualties in all but the most intractable insecure settings.\(^8\)

The policy importance donors place on an agenda sends a message to agencies, especially their executive leadership, as to how much of an organizational priority it should be. Moreover, the lack of active engagement and coordination between donors on security financing can and does have a negative impact on the overall humanitarian response.\(^9\)

Full Spectrum Security Collaboration Mechanisms will foster the horizontal, vertical and diagonal sharing of relevant information and facilitate information and cost sharing for the participating stakeholders.

The diagram that represents the informal, intermediate, and full-spectrum mechanisms can be used as a tool to better evaluate and assist in creating collaborative structures.

The stakeholders can then interpret and compare analysis with their individual Security Risk Assessments in order to adjust activities and/or locations of their programs.

Organizations participating in the collaborative effort will be able to provide a more focused image of the security situation and will assist the NGO in \textit{vertical} and \textit{horizontal} sharing of important information.

\(^7\) ECHO 2006: NGO Security Collaboration Guide. Brussels (by Sean Bickley) and the Good Practice Review on Operational Security Management in Violent Environments: Revised 2010

\(^8\) (HPG Policy Brief 34, April 2009) Providing Aid in Insecure Environments, 2009 Update, Abby Stoddard, Adele Hamer and Victoria DiDomenico

# List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANSO</td>
<td>Afghanistan NGO Security Office</td>
</tr>
<tr>
<td>AWSD</td>
<td>Aid Worker Security Database</td>
</tr>
<tr>
<td>CAP</td>
<td>Consolidated Appeal Process</td>
</tr>
<tr>
<td>ECHO</td>
<td>European Commission Humanitarian Aid Office</td>
</tr>
<tr>
<td>EISF</td>
<td>European Interagency Security Forum</td>
</tr>
<tr>
<td>FTS</td>
<td>UN OCHA Financial Tracking System</td>
</tr>
<tr>
<td>GANSO</td>
<td>Gaza NGO Safety Office</td>
</tr>
<tr>
<td>IASC</td>
<td>Inter-Agency Steering Committee on humanitarian affairs</td>
</tr>
<tr>
<td>IASMN</td>
<td>Inter-Agency Security Management Network</td>
</tr>
<tr>
<td>ICRC</td>
<td>International Committee of the Red Cross</td>
</tr>
<tr>
<td>IED</td>
<td>Improvised Explosive Device</td>
</tr>
<tr>
<td>IFRC</td>
<td>International Federation of the Red Cross and Red Crescent Societies</td>
</tr>
<tr>
<td>ISPO</td>
<td>Information Security Policy of the Organization</td>
</tr>
<tr>
<td>MOSS</td>
<td>Minimum Operating Security Standards</td>
</tr>
<tr>
<td>NCCI</td>
<td>NGO Coordination Committee in Iraq</td>
</tr>
<tr>
<td>OCHA</td>
<td>UN Office for Coordination of Humanitarian Affairs</td>
</tr>
<tr>
<td>SAG</td>
<td>Strategic Advisory Group of InterAction</td>
</tr>
<tr>
<td>SLT</td>
<td>Saving Lives Together</td>
</tr>
<tr>
<td>SMI</td>
<td>Security Management Initiative</td>
</tr>
<tr>
<td>SPAS</td>
<td>Somalia NGO Security Preparedness and Support program</td>
</tr>
<tr>
<td>SRA</td>
<td>Security Risk Assessment</td>
</tr>
<tr>
<td>SRM</td>
<td>Security Risk Management</td>
</tr>
<tr>
<td>UNDSS</td>
<td>United Nations Department of Safety and Security</td>
</tr>
</tbody>
</table>
References

- 66th Working Group Meeting.

Acknowledgements

Michael O’Neill Director of Security, Save the Children
Norman Sheehan Director of Security, AED
Robert Macpherson Cosantóir Group
Trevor Hughes Director of Security, IRD
Tina Westbrock Director of Security, IMC
Chris Williams Director of Security, Plan International
Isaac Evans Director of Security, Children’s Fund
Joe Donahue CEO, iMMAP
Chuck Connolly iMMAP
Dr. Michael Gresalfi DHS
Shawn Bardwell USAID/OFDA
Val Flynn ECHO
Jim Bishop Former Vice President, HPPT, InterAction
Josh Kearns USAID/OFDA
Tracy Jones Intern, InterAction
Robert Painter NGO Liaison, UNDSS
Oliver Behn European Initiative Security Forum

InterAction Security Advisory Group
MINUTES OF THE INGO SECURITY FORUM MEETING

JUNE 17, 2008 AT 10:30 A.M.

Chaired by: Mr. Q

Present:

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Agenda:

Item No.1  Introduction
Item No.2  Review of last meeting minutes
Item No.3  Debriefing by UNDSS
Item No.4  Updates from the Field
Item No.5  Threats to INGOs
Mr. Q, Security Manager, NGO A Pakistan opened the meeting and welcomed the participants. He requested all the participants to share their security information as much as possible so that the feeling of ambiguity could be eliminated and security determined on the appropriate level.

Item No.1: Introduction

Mr. Q introduced himself as the Chair of the Forum and started with the introductions

Introduction of the participants

Item No.2 Review last meeting minutes

The minutes of the last meeting were approved with few a minor changes

Item No.3 Debriefing by UNDSS

The Chair informed the Forum that as the UNDSS representative was not present hence the briefing could not be given.

Item No.4 Updates from the Field

Mr. K shared that the UN offices were closed for the period of one week and no specific reason had been given. Speculation is that the French Cultural Centre had received a threat letter from the Taliban in Afghanistan hence they closed down their office indefinitely. The media had misinformed that all UN offices were closed indefinitely.

NGA B received a threat letter from Khurram Agency that NGO B should not send their female staff to work in the fields. The work is currently suspended. An FIR was lodged however no further action has been reported.

NGO C: Nothing to report

NGO D: Nothing to report

NGO E: Working in NWFP and Sindh areas. After the tragic incident at the NGO A, Area X office, they moved their regional office to Abbottabad. They had also received threat e-mail messages
NGO F: It was reported that there has been a shortage of diesel in Mansehra and Peshawar since last week. It was shared that before / during the announcement of the new budget, gas stations adopt the practice of putting away the commodity for later use at a higher price

NGO G: Nothing to report.

NGO H: Nothing to report

NGO I: Nothing to report. Resuming new program in Peshawar area. Not able to travel to tribal areas to reach the target population due to security reasons.

Private Security Company A: Nothing to report.

NGO J: Nothing to report.

NGO K: It was reported that information could not be communicated between Peshawar and Parachinar. Their training has been postponed due to this reason. Two members from their organization were attacked during their mission. Fortunately none of the staff was hurt.

NGO L: Received a threat email from Balochistan stating not to initiate any programmes in the Balochistan area. A discriminatory note stating that Punjabis were not welcomed.

NGO M: They have restricted their movements in their field areas

NGO N: Mr. Q mentioned he was planning to attend a meeting in Mansehra in order to get an update on the tragic incident of 25 Aug 2008. NGO N had approached various offices like the DCO, DG but the investigation is still on hold. No clear indication for the rationale has been established for this horrendous crime. It was suggested that the Interior Ministry should be contacted to obtain assistance in this regard.

NGO O: Threat received that female staff in Battagram should not work in the fields or hospitals. The female staff has been removed until the elections on 26 June 2008.

NGO P: Work progressing in Punjab and Islamabad areas. No threats. Their security officer is visiting various regions and districts where they are operational to assess and review security conditions prevailing and will report upon his return.

Item No.5 Threats to INGOs

Some organizations have received threats in the last couple of weeks.

Following the bombing in front of the Danish Embassy, where the UN office across the street was also wrecked, there were speculations that maybe the UN office could have been the real target.

There is an open warning from the Al-Qaida that the UN offices will be targeted globally.

It was shared that a technique could be adopted on most mobile phones to block unwanted calls from crank callers.
The Pakistan Telecom Authority (PTA) has come up with a special number where one can register complaints against mobile numbers from which obscene or harassment calls are received. The Number is: 0800-550.

It was also suggested that Cyber Crime Branch or the Interior Ministry could be contacted to determine/investigate the threat call/email received.

The Long March ended peacefully however INGOs were concerned and closed their offices.

Item No.6 Any other business.

Permanent Security Focal Person: Mr. Q shared that it was not possible for NGO B to fund a full time Security Person for the forum as suggested in the previous meeting. He could continue in the capacity as the NGO B Security Coordinator and share the information accordingly. The forum appreciated and lauded his commitment and efforts to act as a Chair at the Forum.

INGOs working without registration: The forum was updated that several unregistered INGOs were compelled to close down their offices in Balochistan area. It was noted that all INGOs are to be registered with the Interior Ministry that would facilitate the INGOs in obtaining the NOC from the Home Department in initiating programs in various provinces in Pakistan.

Focal person to obtain security information from the police: It was suggested to having a focal person (like UN and some of the NGOs) who would visit and obtain security information that could be passed to the INGOs. The NGO C Coordinator informed the forum that the INGOs should observe a low profile with the police and perceived that getting too close to the police might have adverse reactions as they might start dictating and imposing upon the INGOs.

Sectarian violence in Hangu area: Four Shias were shot dead and random firing was reported. Kohat roads was blocked so that the Sunnis could not cross and start another sectarian feud. Hangu Bazar was closed down due to security reasons. In Dera Ismail Khan, four children were shot during the sectarian feud and the bodies were taken to Kotri for burial.

One day workshop: It was suggested that the Forum needs to conduct a one-day workshop so that everyone can be brought up to date on the current security situation. Each organization willing to participate could pay for their own representative and the workshop could be held at Serena Hotel or either in Murree or Nathiagali.

In-active members of the forum: It was suggested to encourage the inactive members to participate. Another proposition was to have an alternate person attending the meeting so that the information is conveyed to the organizations accordingly. Members that have discontinued their participation or are not interested should inform the INGO Security team of their withdrawal from the forum.

Item No.7 Announcement of next meeting:

The INGO Security Forum meeting was concluded with a thank you to all the participants. The next meeting will take place on Tuesday, July 1, 2008 at 10:30 a.m. at the NGA A
PARTICIPANTS: MSF-B, MSF-H, ACF, MERCY CORPS, COORDAID, TEARFUND, ACT Alliance, ACTION AID, SC-UK, CARE, ISLAMIC RELIEF, JEN, RELIEF INTERNATIONAL, HI-B, GOAL, CONCERN, REDR-BIOFORCE, HAVEN, HELPAGE INTERNATIONAL, AMI, ACDI-VOCA, IMC, CRS, OXFAM GB, IRC.

1. INTRODUCTION - ROUND TABLE

2. JMAC UPDATE

JMAC reported on last week-end Police operations: United Nations peacekeepers helped PNH capture 30 criminals who had escaped from prison and subsequently infiltrated a camp for internally displaced persons (IDPs).

More than 350 military and police staff serving with the UN Stabilization Mission in Haiti (MINUSTAH) raided the Jean-Marie Vincent camp for IDPs near the notorious Cité Soleil neighbourhood of Port-au-Prince shortly after 5 a.m. the raid was conducted following an upsurge in violence inside the IDP camp that was linked to the prison escapees.

JMAC confirmed that Gangs reorganised in Martissant and are more active since the last three weeks. It has been motioned that this Gangs have links within local Police, and pointed out the differences between street gangs in Martissant and armed group in Cite Soleil.

JMAC reported that NGOs are now receiving “Yellow and Red Card”, that will grant them access or not in some area.

This is also confirming recent reports from NGOs encountering difficulties working in this neighbourhood and this since the last 3 weeks.

3. INCIDENTS REPORTS

18 June 2010 – Antigovernmental protests. 4 assembly points (Carrefour, Petionville, Pl Jeremie, St Jean Bosco)

18 June 2010: The Haitian police have launched the last weekend a series of operations. In 72 hours 3 interventions were conducted in the area of Mapou Fontamarra to 27 in Saline and in two shelters in Delmas.23/06/2010 JHSF Minutes of Weekly Security Meeting

21 June 2010 - PNH also launched operation in Martissant 17, reports of several people killed or injured.
20 June 2010 - Violent demonstration in Ghantier on the way to Dominican Rep. Demonstrators attacking local Police station with stones. 8 shots were fired.

21 June 2010 – Demonstration reported down town (Bois Verna, Av La Martinire) and JP II near Ministry of Justice

An NGO reported armed robbery in front of the maternity hospital Isae Jeanty. It has come to the conclusion that such incidents are frequents in the area.

It has also been reported that Gangs are equipping youngster with arms, to work for them and bring back cash.

Report from an NGO:

“One of our Haitian NGO partners work and live in the Petion area of the Champs de Mars IDP Camp. They are mostly women and work on Gender Based Violence (GBV) issues. On Thur 17 Jun a single individual with a weapon (which he did not pull out to threaten anyone) came asking for money and help saying he deserved attention as well, and that he knew ‘foreigners’ were helping this NGO. One of the NGO staff placated him with 500 Gourdes, but he stayed with them though did not threaten anyone. The staff went away on Fri and Sat. When some of the women came back on Sat night, he was waiting with others who demanded money and threatened to shoot them (all of them armed). They had been waiting for the women to return all day and they were armed. Some of the neighbours helped the women to escape, and they are now at a different location.

What is clear was that these men had watched these NGO staff and saw that an INGO was helping them, and therefore assumed they had money. We are now meeting with our local NGO partners in 3rd party locations to avoid a repeat of this incident.”

4. JHSF Update:

Funding & Proposal

The initial project and funding (ECHO) ends on 22nd of July 2010, and in order to ensure the continuity of JHSF activities and services, a new proposal has been drafted and introduced for consultation with the Forum Members.

The future activities and project outlines are as follow:

Project Title: Provision of Security Coordination for NGOs operating in Haiti

Principal Objective

To facilitate the efforts of humanitarian organizations to operate in a secure manner while conducting assistance activities to benefit the disaster-affected population23/06/2010 JHSF Minutes of Weekly Security Meeting

Specific Objective:
To improve the flow of important and relevant information among NGOs to help them to manage the security of its staff and assets.

Result 1: Increased exchange of information-security-within NGOs

Activities:

Regular Security meetings of member NGOs and observer NGOs
- Weekly in Port au Prince
- When necessary in the in the provinces

Weekly report of meetings and activities of relevance to NGO activities in Iraq

Routine and specific security reports for JHSF members and other involved actors- UN, donors –including a weekly data extraction on security incidents

JHSF SA attendance at Steering Committee meetings, ad hoc meetings on relevant topics- operational and security

Updating of the JHSF databases

Continuous updating of JHSF contact lists and emergency list

Continued additions to JHSF library of reference materials

Development of a mapping system

Regular review of local press and dissemination of relevant articles (translated if appropriate)

Result 2:

Improved security liaison between NGOs and third parties- UN agencies, Haitian Authorities, Donors, security providers.

Activities:

Ad hoc meetings with third parties- UN, Iraqi authorities, donors, security providers.

Transmission of material relevant to humanitarian activities and to security management for NGOs with activities in Haiti.

Preparation with the NGOs of letters and statements on specific security issues.

In conclusion The Forum expressed the need of the JHSF not only to continue its activities but also to increase its capacity and geographical coverage in order to provide similar services for NGOs throughout the country.

JHSF could establish a network with identified geographical security focal points with punctual visits and support from JHSF.23/06/2010 JHSF Minutes of Weekly Security Meeting
5. AOB

Contingency Planning Work Group

Following a discussion in the meeting, it was agreed that we’ll investigate the viability of holding a workshop aimed at assisting members in the preparation of a Disaster Preparedness Plan for their own staff.

An initial discussion as to how this could be taken forward has been scheduled with a representative forum of 6 persons. A feedback is expected during the next Security Meeting

Emergency Telecommunications

It has also been proposed to do a mapping of the existing communications networks and capacity. This information will be collected by JHSF via a form that will be circulated shortly.

JHSF Membership:

JHSF will prepare and circulate a new form for registration purpose; including lists of contacts, call signs, GPS coordinates offices outside PAP, etc. This will allow us to keep our contact list up to date and gather important information for later mapping.

*****

The next meeting is schedule on Wednesday, June 30th, 12am - held in the RedR-Bioforce Meeting Room.
Annex 3 – SPAS (Full Spectrum – Weekly Report)

ABBREVIATED

Somalia NGO Security Preparedness and Support Program (SPAS)

Report Number – 22/08

Reporting Period:

21st – 27th May 2008

Notes

1. The Security Preparedness and Support (SPAS) Program is a concept of the Somalia Non-Governmental Organizations Consortium whose only concern is the safe provision of humanitarian and development Aid to the people of Somaliland and Somalia, therefore SPAS is an NGO project dedicated to the safety and security other Somali NGO Consortium members

2. SPAS is non-governmental. The SPAS Security Report is for the use of the Somalia NGO Consortium. The aim is to provide neutral and transparent information to facilitate security decision-making by Consortium members. SPAS assumes no responsibility for report accuracy, reliability or verification unless stated.

3. This report is the latest update on available security related information in Somalia and Somaliland. Situations may have changed and / or will change.

4. SPAS recommend that the NGO community use all best and available sources of information.

5. Security decision-making and protocols are the responsibility of subscribing NGOs. Security precautions are recommended at all times in accordance with respective organizational procedures.

6. SPAS does not provide security alert levels. The identification and provision of security alert levels/phases/thresholds are the responsibility of each individual organization.

7. This report is distributed for the information and benefit of the Somalia NGO Consortium.
The sole purpose of the threat map below is to visually represent heightened areas of concern for humanitarian actors. The map represents only the opinion of NGO-SPAS staff and therefore is by no means comprehensive. Service users should acknowledge that this representation is only as good as information received from actors on the ground. Therefore, agencies with specific information regarding the threat in a particular area are encouraged to contact SPAS for the benefit of all humanitarian actors working in Somalia and the Somali people.

Executive Summary

The reconciliation effort to mediate between the “Alliance for the Liberation and Restoration of Somalia” (ALRS) and the TFG are expected to continue from 30th May, 2008 in Djibouti. Despite a preliminary first round of talks between the ALRS and the TFG earlier this month, the two sides remain profoundly hostile to each other and the risk of armed confrontation remains high in the foreseeable future.
Banadir, Middle and Lower Shabelle Regions:

The security situation once again deteriorated over the reporting period with insurgent attacks against TFG and its allies intensifying throughout central and southern Somalia with a profound number of casualties. Multiple attacks by AOGs against AMISOM, ET and TFG troops continued in Mogadishu city. The police commander for Lower Shabelle regional Division reportedly survived a landmine attack with TFG police attacked with a landmine in Medina. A Kenyan lecturer held hostage was released, nevertheless four other Internationals are reportedly being held within Mogadishu. Insurgent’s attacks against TFG and its affiliated troops are expected to continue within the regions.

Bay and Bakool Regions:

Tension remained high amongst the local population following the increased movements of AOGs who have seized control over all main strategic areas of Bay and Bakool regions except Baidoa town. There is a large contingent of insurgents within Baidoa who are expected to carry out more insurgency activities as declared by their leaders. IEDs and grenade attacks have become a common occurrence against ET/TFG forces. Incapacity of Government security forces to control the situation has led to gradual deterioration of security situation in the region with expansion of ICU/Al-Shabaab influence. Insurgents are reportedly issuing threat letters advising the local population to avoid Baidoa town due to imminent engagements with ET/TFG forces.

Hiraan and Galgadud Regions:

In Beletweyne town, AOG militias hurled a hand-grenade against ET troops prompting them to retaliate with heavy fire power. The local population has been exercising extreme caution due to fear of being caught in crossfire. There are reports that AOGs will be announcing independent administration in Bulo-Burte town against the TFG. In connection with this new dynamic ambush attacks against ET/TFG troops are expected to continue in the coming weeks despite heavy presence of ET troops. Galgadud region remained volatile with systematic assassinations, clan clashes and a piracy related incident where al-Shabaab militias engaged pirates after the ship was released.

Gedo, Middle and Lower Juba Regions:

The security situation remained calm in Gedo, parts of Middle Juba but tense in Lower Juba region. Reportedly Marehan clan and the ICU militants met and agreed that insecurity in Kismayo must be addressed at once. The aid community has come under intense pressure notably with LNGO staff being targeted reportedly for being suspected to be working as spies. In addition to clan related militia and ICU activities the GU rains in Middle and Lower Juba regions have made roads impassable. The aid community should plan carefully any convoys in these regions.

Following several towns takeover, ICU has scored a decisive victory against TFG within Lower Juba and established itself as the dominant authority throughout much of southern Somalia. Sources close to AOGs from Jilib District indicate that ICU was allegedly called upon to solve political differences between the Asmara group and the Al-Shabaab over Jilib and Kamsuma towns with reported death threats for any person appointed by either group. The prospects for a bitter showdown among the
AOGs based in the area remain very real. This is assessed to affect the security situation in the entire region as echoed by AOG leader that they will fight and ensure all foreign forces leave Somalia.

Puntland:

The establishment of Puntland Security Management team, also known as the “Security Core Group”, comprising representatives from UN, INGOs, Minister of Security, Minister of Interior, Elders and Community Policing is a positive step towards security of the aid community. However, the presence of armed militiamen inside Bossaso and Galkayo has notably increased levels of insecurity in the towns during the reporting period. Law enforcement authorities continue to be targeted by armed militias with IEDs and assassination attempts. It is assessed that AOGs are setting foothold in the region in connection with the fighting between AOGs and clan militias in South of Mudug region. This will have a profound impact on security in Puntland in the foreseeable future.

Somaliland:

The security situation in Somaliland remained calm with meetings between the government and the opposition parties allegedly solving the electoral related dispute which has been continuing during the last two months. A landmine blew up a vehicle killing five passengers which underscores the potential danger landmines still pose in the region. The aid community is advised to take precautionary measures in all regions that have not been declared mine safe.

Statistical Data:

The statistical data below represent security incidents reported by NGO SPAS from 1st January 2008 to the 27th May 2008.

PRP: AOG Attack: 20 May 08, 17:00hrs, Siinka-Dheer (KM18), Mogadishu: 30 armed men attacked a TFG police check point located at KM 18 Southwest of Mogadishu (border between Mogadishu and Afoi town). The AOGs took over control of the check point for about half an hour.

PRP: RCIED Attack: 20 May 08, day time, Former Jaalle Siyad Military Academy, Hodan District: A roadside RCIED constructed from a land mine detonated in close proximity to ET and TFG forces
while conducting patrol along the above mentioned location. During the incident 2 TFG and 2 ET troops were killed.

PRP: Mortar shells Attack: 20 May 08, day time, Former defence Headquarters, Guulwadaaasha, former Spaghetti factory and Haile Barise buildings, Hodan and Yaqshid Districts: AOG fired 6 mortar rounds.

Assassination: 21 May 08, 08:30hrs, Medina Market, Medina District: Unidentified men armed with pistols.

Mortar Attack: 22 May 08, 18:00hrs, Former Spaghetti factory, Yaqshid District:

Assassination: 22 May 08, 18:20hrs, Bakara Market (Abu-Hureyra Mosque), Howlwadag District: A man was found dead

Hand Grenade Attack: 23 May 08, 11:45hrs, Banadir Secondary School, Hodan District: AOG hurled a hand grenade

RCIED Attack: 23 May 08, 12:00hrs, road between Km4 and Aden Adde Int. Airport, Medina District: A roadside RCIED constructed from a landmine detonated

Hand Grenade Attack: 23 May 08, day time, Florence hotel road junction, Wardhigley District: AOG launched a hand grenade attack

Mogadishu reportedly 4 TFG police were killed, 5 TFG police taken as hostages and robbed of tax money collected. enforcement arrived in the area and conducted house to house search in nearby areas arresting suspects. over mentioned locations reportedly killing one ET soldier at e former Ministry of Defence headquarters. district: Unidentified men hurled a hand grenade against TFG police base, no casualties were ported. shot and killed Mr.Abdullahi Mohamed Ali inside his store; reason behind the killing remains unknown. mortar shells and RPG-7s. One mortar shell landed at African village (Hodan District) killing an old man. AOG launched mortar attacks against ET troops prompting a fire exchange, no casualties were reported. 6 men armed with pistols shot and killed him. The motive behind the killing has not been established. against TFG and ET troops conducting patrol in the area; during the incident 2 civilians were wounded y to AMISOM envoy (Ugandan troops); during the incident 4 Ugandan soldiers were reportedly injured. ck against TFG forces based at the above mentioned caution; both sides exchanged small arms fire.
Annex 4 – Levels of Collaboration

The question of collaboration should not be either one does or does not participate. If we identify collaboration on a continuum with independence on one end and collaboration on the other, we can then break down collaboration into different levels each having basic characteristics.

Characteristics

- **Registration**: Organization may be in the ‘receive’ mode.
- **Information Sharing**: Organization shares information and attends meetings.
- **Participation**: Organization hosts collaborative mechanism and values full participation.

InterAction Security Collaboration Self-Test

(following page)

**Instructions**: Select the statement which best describes your collaboration activities and place the corresponding value to the in the box on the right. Total the score to and compare it to below.

<table>
<thead>
<tr>
<th>Registration</th>
<th>9 – 13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Sharing</td>
<td>14 – 20</td>
</tr>
<tr>
<td>Participation</td>
<td>21 – 27</td>
</tr>
</tbody>
</table>
### InterAction Security Collaboration Self-Test

<table>
<thead>
<tr>
<th>Contribute</th>
<th>Registration</th>
<th>Information Sharing</th>
<th>Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research &amp; Gather Information</td>
<td>Does not collect any information</td>
<td>Collects very little information</td>
<td>Collects a great deal of information—all relates to the topic.</td>
</tr>
<tr>
<td>Share Information</td>
<td>Does not relay any information</td>
<td>Relays very little information—some relates to the topic.</td>
<td>Relays a great deal of information—all relates to the topic.</td>
</tr>
<tr>
<td>Participation</td>
<td>Does not</td>
<td>Occasional</td>
<td>Fully</td>
</tr>
<tr>
<td>Fulfill Team Role’s Duties</td>
<td>Does not perform any duties</td>
<td>Performs very little duties</td>
<td>Performs all duties of assigned team role.</td>
</tr>
<tr>
<td>Participate in Conference</td>
<td>Does not speak during the conference.</td>
<td>Either gives too little information or irrelevant information.</td>
<td>Offers a fair amount of important information—all is relevant.</td>
</tr>
<tr>
<td>Share Equally</td>
<td>Always relies on others to do the work.</td>
<td>Participates—often needs reminding.</td>
<td>Always participates without having to be reminded.</td>
</tr>
<tr>
<td>Listen to Other Teammates</td>
<td>Usually doing most of the talking—rarely allows others to speak.</td>
<td>Listens, but sometimes talks too much.</td>
<td>Good and productive balance of listening and speaking.</td>
</tr>
<tr>
<td>Cooperate with Teammates</td>
<td>Usually argues with teammates.</td>
<td>Rarely argues</td>
<td>Never argues with teammates.</td>
</tr>
<tr>
<td>Make Fair Decisions</td>
<td>Usually wants to have things their way.</td>
<td>Often sides with friends instead of considering all views.</td>
<td>Always helps team to reach a fair decision.</td>
</tr>
</tbody>
</table>

---

**Annex 5 – SLT Revision Report**

(See following 11 pages)
IASC STEERING GROUP ON SECURITY – SAVING LIVES TOGETHER TASK FORCE

REPORT ON THE REVISION OF SAVING LIVES TOGETHER

Executive Summary

1) Working under the oversight of the IASC Steering Group on Security (SGS), the Saving Lives Together Task Force (SLTTF) was charged with the revision of the Saving Lives Together (SLT) document and the development of short and long term plans to effect the institutional arrangements deemed necessary to the revitalization of SLT. The SLT Task Force undertook a series of fortnightly meetings, beginning on Friday, 12th March 2010, with the aim of preparing a first draft of the SLT revision and a road map for implementation of the institutional arrangements for the review of the SGS. While the SLTTF began with a composition of UNDSS, OCHA, EISF, ICVA, InterAction and SCHR, with the concurrence of the SGS, the group invited UNICEF and WFP to round out the group with additional expertise.

2) The SLTTF, guided by the findings and recommendations of a number of surveys and studies on the subject of UN and NGO security collaboration, identified reoccurring hurdles to SLT implementation, including lack of clarity over roles and responsibilities, the requirement for dedicated resources and coordination, and confidentiality issues. Thus the aim of the revision of the SLT Framework has been twofold: to streamline and simplify the recommendations to six clearly defined areas of focus, and to provide a staged approach to implementation, which defines who does what, when and how, with a focus on triggers for implementation based on agreed IASC mechanisms such as the Sub-Working Group on Preparedness and Contingency Planning’s Humanitarian Early Warning Service and the Sub-Working Group on the Consolidated Appeals Process.

3) The SLTTF, recognizing the recent developments in security management - in particular in terms of information based and contextual security risk assessment methodology - has sought to inject SLT with a reinforced approach to the conduct of contextual, agency and programme specific risk analysis (SRA), which will establish common and individual risk profiles. The SLTTF recognizes the efforts of DSS in terms of SRA, and also notes the alternate utility of the ISO 31000 - Risk Management Process, as an international industry standard applicable to the situation and acceptable to all parties. While individual risk profiles will differ, there may be opportunities for a common approach to SOPs between UN agencies and NGO/IOs which should be operationalized, taking into consideration existing efforts. A viable basis for a shared approach to security information management, including a common lexicon, has been identified by the SLTTF that being the UNDSS approach to Security Threat Information (STI), which can be adapted for the benefit of the humanitarian community.

4) Means of propagating the revised SLT are addressed through the reinforced institutional arrangements, global and country level security training initiatives, and by the proposed piloting of SLT in predetermined locations. To ensure buy-in from all constituents, the institutional home of SLT remains the IASC, however the SLTTF identified the requirement for an IASC SLT coordination resource, such as the current IASC Steering Group on Security, to implement the
recommendations contained herein (in particular those that require long range investment such as reinforced risk management approach and security training initiatives), and to ensure momentum is maintained and that best practices are collected, analysed and disseminated in a manner similar to other IASC products. At the country level, there is an urgent requirement for dialogue on security matters at the professional level in the field, which should be addressed in the context of a local joint Security Working Group, comprised of UN and NGO security personnel, which would provide an effective framework to support joint security programmes and proposals. The United Nations Security Management System and DSS in particular must take the initiative on the revised SLT, to overcome the reoccurring hurdles to implementation.

5) The security training element was most advanced prior to the formation of the SLTTF, as there was a long-standing proposal for a joint UN and NGO security training CD-ROM or internet-based application for operating in high risk environments. The SLTTF fully supports this initiative and will contribute to it realization, while at the same time working with DSS and INGO security training providers to ensure that the revised SLT, including the new security risk and information management approach, are incorporated in all staff and security officer training platforms. The training programme should have a dual focus, to calibrate extant SLT initiatives in line with the revised approach and to initiate SLT arrangements in countries with little or no SLT activities, selected through a representational process. As such the preliminary list for piloting of the revised SLT Framework would include Afghanistan, DRC, Haiti, Chad, and Pakistan, as well as emerging crises in which the SLT model should be implemented from the onset of the crisis.

6) The recommendations of the SLTTF will require considerable donor support to be effective. While expertise is available, lack of resources has been the major impediment to SLT implementation. Surveys\(^1\) have shown that security is the least funded sector in the Consolidated Appeals Process and remains the most difficult subject to broach with member states hosting humanitarian operations. In light of these factors, a radical approach is required to revitalize the security regime for humanitarian operations. To this end the SLTTF recommends a much more robust engagement of donors and donor coordination mechanisms including diverse funding streams and access to the CERF as well as the establishment of a prorated approach to security in CAPs or other funding mechanisms to ensure the availability of urgent security requirements.

\(^1\) See Annex: Supporting security for humanitarian action: A review of critical issues for the humanitarian community (a study by Abby Stoddard and Adele Harmer, humanitarian outcomes) a Background document commissioned by the conveners for the Montreux X Retreat on the Consolidated Appeal Process and Humanitarian Financing Mechanisms (18-19 march 2010)
1) **SLTTF Terms of reference and methodology:**

Working under the oversight of the IASC Steering Group on Security (SGS), the Saving Lives Together Task Force (SLTTF) was charged with the revision of the Saving Lives Together (SLT) document and the development of short and long term plans to effect the institutional arrangements, deemed necessary to the revitalization of SLT.

Specifically, the SLTTF was tasked to:

- **Revise Saving Lives Together** – Revise SLT in accordance with SGS timeframe, ensure the introduction and application of risk assessment and management and a model for determining acceptable risk as core elements, as well as respect for individual mandates and approaches. Work with the IASC to ensure appropriate SLT roll out in UN languages and with full guidance package, similar to other IASC products.

- **Identify and develop SLT institutional arrangements** – Identify an appropriate institutional home for SLT acceptable to all stakeholders, i.e., IASC, IASMN, hybrid, etc., and reassess placement of security within the appeal cluster system based on education cluster model (already exists in common services) and make recommendations for inclusion of SLT arrangements in future Appeals.

- **Develop an SLT Funding Base** – seek to widen SLT donor base, find new sources of funding for the long range and set up, between OCHA and DSS, a mechanism for managing donor contributions for SLT. Work with Member States to develop a group of ‘Friends of SLT’. The funding strategy should accommodate the following objectives:

- **Develop an SLT Information Management Approach** - Identify barriers to confidential and sensitive information sharing and review/revise information sharing protocols for improvement and to ensure protocols encompass analysis and crisis management. Assess ongoing efforts and make recommendations on the establishment of a common lexicon for incident/info exchange especially incident and geographical information.

- **Piloting and facilitating SLT** - While underscoring that the responsibility for SLT lies with field practitioners, in certain situations, such as emerging or extremely complex crises, a more robust approach may be required. To this end, the SLTTF should assess and recommend pilot applications for country level SLT.

- **Security training in support of SLT** - Work closely with the IASMN, to develop a “third generation” of CD training for hostile environment applicable to both UN and NGOs, develop SLT roll out dissemination/training module for UN/INGO use, optimally for delivery by NGOs in DSS SCP training and delineate possibilities for exchange of UN/NGO trainers and training modules. Improve extant UN and NGO security training to further promote SLT.
**Methodology:** The SLTTF identified areas of convergence in the findings and recommendations of a number of surveys and studies on the subject of UN and NGO security collaboration. These include in chronological order:

A. IASC paper from 2006, Saving Lives Together, a Framework for improving security arrangements among IGOs, NGOs and UN in the field

B. Study undertaken by the NGO IMC on Security Management in Humanitarian Agencies

C. June 2009 Survey on Saving Lives Together undertaken by DSS

D. Paper produced by InterAction Security Unit, entitled Security Collaboration, Good Practises

A. The eldest of these documents, the IASC paper from 2006, attributed the lack of implementation of the SLT forerunner - the “Menu of Options” - to a number of “reoccurring hurdles” and made a series of recommendations to address such obstacles:

- Competing Priorities and Time Constraints
- Confidentiality issues
- Diversity of Security Approaches
- Lack of Resources

B. The IMC survey revealed: Around 97% of the respondents felt that information sharing was an important area and around 75% felt that joint donor advocacy was also important. Information sharing and joint donor advocacy were seen as the most important areas for NGO security collaboration.

C. The DSS SLT survey assessed:

- A robust and widespread dialogue over the utility and value of SLT.
- Long-standing confusion over roles and responsibilities which have hindered implementation at the strategic level.
- Requirement for dedicated resources and coordination to progress the SLT framework at the tactical level.
- Information sharing, joint training and the inclusion of NGO security personnel in the UN Security Cell is seen as particularly valuable by all concerned parties.
- A number of responses noted how SLT best practices are built on experience in other theatres, which indicate that SLT has become a standard element of the humanitarian toolbox.
D. Findings from the paper produced by InterAction Security Unit, indicate the importance of SLT in terms of:

- Information sharing.
- Opportunities for joint donor advocacy.
- Opportunities for enhanced joint training.
- Inclusion of the NGO security personnel in the UN Security Cell.
- Addressing financial issues related to security.

Findings - The SLTTF, guided by the findings and recommendations emanating from the above-noted surveys and studies on the subject of UN and NGO security collaboration, identified reoccurring hurdles to SLT implementation, including lack of clarity over roles and responsibilities, the requirement for dedicated resources and coordination, and confidentiality issues which hinder the flow of information. While the attempt in 2006 to reinforce UN and NGO security collaboration, which led to SLT, came to similar conclusions, it did not actually prescribe responsibility for SLT implementation. The current revision adopts a practical hands-on approach with clear measurable roles for all parties. Thus, the aim of the revision of the SLT Framework has been twofold: to streamline and simplify the recommendations to six clearly defined areas of focus, and to provide a staged approach to implementation, which defines who does what, when and how, with a focus on triggers for implementation based on agreed IASC mechanisms such as the Sub-Working Group on Preparedness and Contingency Planning’s Humanitarian Early Warning Service and the Sub-Working Group on Consolidated Appeals Process.

2) The Revision of Saving Lives Together

SLT Recommendations: The SLTTF proposes six phases as opposed to the previous ten, primarily on the basis of demonstrated utility. The reduction to six recommendations reflects a streamlining of the originals by merging similar objectives with a greater emphasis on the role of all SLT partners and their respective methodologies contributing to an information-based security collaboration process benefiting the broader humanitarian community. This implies reinforced engagement and understanding of SLT among all partners. For the UN, this comes at a unique time when the UN security management system is clearly evolving rapidly and to which SLT will link effectively, to provide less UN-centric models for the safe conduct of multi-dimensional humanitarian operations. The clear, concise recommendations are complemented by a Staged Approach to SLT implementation with pre-identified triggers for action and a description of the information and collaboration requirements of each stage. The revised Recommendations are as follows:

1) Convening broad-based forums for field security collaboration and information sharing, including NGO/IO engagement with the UN Security Management Team

2) Meeting Common Security-Related Needs and Sharing Resources, including the presentation of mutually identified common security requirements in the Consolidated Appeals or other fundraising mechanisms
3) Facilitating Inter-Agency Emergency Telecommunications

4) Collaborating and consulting on the development and delivery of contextually based security training

5) Identifying minimum security standards on the basis of agency or organisation-specific SRA model

6) Seeking adherence to Common Humanitarian Ground Rules (CHGR)

An information-based and Staged Approach to implementation - To complement the revised recommendations, the SLTTF proposes an information-based and staged approach to UN/NGO/IO security collaboration with clearly defined roles and responsibilities. To the extent possible, SLT functions should be included in training activities, job descriptions and evaluations.

Information based decision making - The reinforced focus on information, may be described as a process in which the humanitarian community collectively defines the requirements for, and contributes to the collection, dissemination and effective management, including confidentiality, and analysis of critical security and safety information and commensurate levels of risk, with the aim of enabling effective programme delivery. The results of the collective information and analysis shall be made available to humanitarian security managers in the interest of our mutual safety. However, all decisions made, on the basis of, or with consideration to, such actionable information remains the prerogative and responsibility of their respective organisations.

As with the other elements of the revision, the approach to implementation of recommendations towards information-based decision making has implications at global and local levels. The global commitment to information-based collaboration has never been stronger than at present; however there remain serious obstacles in the field demanding a concerted effort including training, advocacy, trust-building and field animation. A common framework for incident analysis remains elusive but it is evident from initiatives in this direction that a common approach to security terminology is the most effective basis for collaboration in information sharing. To this end the SLTTF endorses the DSS Security Threat Information (STI) framework (outline attached as an Annex) as the most viable option for delineating a common lexicon for security information, and has initiated a preliminary survey of NGOs which indicated a positive response to this recommendation.

The SLTTF identified the pressing need to define who does what, when and how, with a focus on triggers for implementation based on agreed IASC mechanisms such as the Sub-Working Group on Preparedness and Contingency Planning’s Humanitarian Early Warning Service and the Sub-Working Group on Consolidated Appeals Process. To this end, the SLTTF identified three stages of SLT implementation: Informal, Intermediate and Full Spectrum based on the information required to undertake informed security decisions in a complex operational environment as delineated in the following table:
The SLTTF proposes an information-based and staged approach to UN/NGO/IO security collaboration with clearly defined roles and responsibilities. To the extent possible, SLT functions should be included in job descriptions and evaluations. To ensure buy-in from all constituents, the institutional home of SLT remains the IASC, however the SLTTF recommends a long term SLT coordination resource be established under IASC, to ensure the following SLTTF recommendations are achieved and best practises are collected, analysed and disseminated.

<table>
<thead>
<tr>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ten original SLT recommendations have been distilled to six essential objectives</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Informal Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early warning/crisis prone Country listed on IASC Early Warning list is the trigger for SLT implementation</td>
</tr>
</tbody>
</table>

**Information Requirement:** The humanitarian community contributes to the collection and dissemination of critical security and safety information. Information and analysis is thus made available to humanitarian security managers in the interest of our mutual safety and all decisions made, on the basis of, or with consideration to, such information remains the responsibility of their respective organisations.

<table>
<thead>
<tr>
<th>Intermediate Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mounting or low intensity crisis – Country identified as in crisis and eligible for CAP or other funding mechanism for humanitarian intervention</td>
</tr>
</tbody>
</table>

**Information Requirement:** Systematic collection of incident reports and open source analysis. Regular trend analysis, coupled with basic scenario forecast. UN security cell and/or INGO safety coordination platforms will provide the forum for joint analysis.

<table>
<thead>
<tr>
<th>Full Spectrum Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open conflict/disaster – ongoing CAP or other humanitarian funding mechanism, massive crisis response/unmet identified need in insecure environment May include DPKO mission with Humanitarian mandate</td>
</tr>
</tbody>
</table>

**Information Requirement:** SIOC quality detailed trend analysis on a monthly, quarterly, seasonal or as required basis, providing a comprehensive threat image including forecast that is often broken down by regions. SIOC or security cell and/or NGO safety coordination platform provide the forum for joint analysis.

1) Convening broad-based forums for field security collaboration and information sharing, including NGO/IO engagement with the UN Security Management Team

Whether the forum is UN or INGO, the critical requirement is to create the space for a robust dialogue on security collaboration.

Plug into DSS training unit and NGOs doing training

| UN DO must ensure fora for security collaboration among all humanitarian actors at area, country and sub-office level are convened, at regular intervals, to address practical security issues of common concern – DO/HC NGO/IO SFPs |
| DSS engages NGO/IO security personnel in UN Security cell or UN participates in NGO safety coordination platform |
| DO ensures that SLT is a agenda item at UNSMT & consideration given to inviting Senior Managers of the NGO/IOs to attend relevant portions of SMT meetings or that such security coordination requirements are met in other fora. |

| SLTTF support and monitoring, identification and compilation of best practises and strategies |
| Frequency increases to monthly or as required |
| SLTTF supports country level efforts |
| Regular NGO/IO participation in UN security cell or UN in INGO safety coordination platform support and guidance |
| NGOs and the Red Cross Movement may participate in relevant meetings of the UN SMT on an ex-officio basis. |

---

2 Ex officio here refers to the fact that representatives of non-UN organizations are not bound by, nor participate formally in, SMT decisions on UN security policy.
## 2) Meeting Common Security-Related Needs and Sharing Resources, including the presentation of mutually identified common Security requirements in the Consolidated Appeals or other fundraising mechanisms

**Ensure coordinated approach meeting communities’ needs not just one by one**

**Prioritize field requirements**

<table>
<thead>
<tr>
<th>Preparation Stage</th>
<th>Appeal or other funding means preparation – Security Cell with NGO/IO input or INGO safety coordination platform support and OCHA CAP guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory of security requirements DSS/NGO/IO SFPs</td>
<td>DO/HC ensures humanitarian coordination system includes Security component – security cell and/or INGO safety coordination platform support and guidance - HC/DO/NGO/IO SFPs, backstop at HQ by the SLTTF</td>
</tr>
<tr>
<td>Potential security requirements identified in advance on basis of early warning scenario, i.e. natural disaster, conflict, etc.</td>
<td>Optimally the Security Cell and/or INGO safety coordination platforms defines the security requirements, otherwise an ad-hoc group should be convened</td>
</tr>
<tr>
<td>Liaison with Host Gov on preparations as required – DO in concert with HC, HCT, NGO/IO SFPs</td>
<td>Donor liaison by DO/HC/NGO/IOs on security needs</td>
</tr>
<tr>
<td>SLTTF engage IASC Early Warning and OCHA regarding potential Appeals &amp; alert field</td>
<td>Prioritize requirements &amp; develop protocols for resource sharing - Security cell and/or INGO safety coordination platform support and guidance with SLTTF backstopping</td>
</tr>
</tbody>
</table>

### Ongoing Appeal or other funding means with well conceived and developed UN/NGO/IO security projects within CAPs to cover the additional resources potentially required for enhanced collaboration on staff security by UN Agencies and NGO/IOs, such as telecommunications and security training.

- Security cell and/or NGO safety coordination platforms support with SLTTF backstopping
- Constant assessment and re-evaluation of requirements reflected in Appeal or other funding mechanism - Security cell and/or INGO safety coordination platform support with SLTTF backstopping

## 3) Facilitating Inter-Agency Emergency Telecommunications

**Focus on Inter-operable integral systems**

| The DO advocating with the relevant authorities for the use of telecommunication equipment within the framework of existing international agreements; | The relevant UN body, usually DO, negotiating with the authorities a common, inter-agency frequency to facilitate greater interoperability for security collaboration for UN organizations and NGO/IO operating |
| SLTTF HQ link with UNHAS and Fittest, TSF to pre-arrange coordinated approach | Support the requirement for the communities common and in-house communications infrastructure |
| CAP or other funding means proposal for requirements – Security cell and/or INGO safety coordination platform support and guidance with relevant agency/org representation | DO/UNSMT or other liaise with UNHAS and FITTEST |

### Humanitarian actors committing to security collaboration using standard communication procedures and, to the extent possible, providing staff with compatible communication systems

- UN advocates for licences and frequencies granted and maintained
- Operating CAP or other funding means project providing services to UNHCT

## 4) Collaborating and Consulting on the development and delivery of contextually based Security Training

| Observe and share training materials and requirements with focus on preparedness and specific context – DO/FSCO, NGO/IO SFPs | Seek to increase their capacity for security training at all levels & when feasible, pool necessary resources to conduct field security training – DO, NGO/IO SFPs, NGO security trainers, Security Cell and/or INGO safety coordination platform. |
| Give consideration to the development of training that | Maintain all previous initiatives |
| | Carry out joint security training in collaboration and/or consultation with other agencies to the extent possible – Security Cell and/or INGO safety coordination platform support and guidance |

### Humanitarian actors committing to security collaboration using standard communication procedures and, to the extent possible, providing staff with compatible communication systems
<table>
<thead>
<tr>
<th><strong>Generation III CD-ROM and internet based application for both UN and INGOs operating in high risk environments to address global requirements, supported by contextual initiatives at country or local level</strong></th>
<th>focuses specifically on improving security collaboration – CSA/FSCO/NGO/IO Security trainers</th>
<th>Additional training resources, such as DSS Field Support Service and/or security training. NGOs contribute to ensure efficacy of contextual training</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5) Identifying Minimum Security Standards on the basis of Agency or organisation-specific SRA model</strong></td>
<td>In recognition of the fact that programme and security are linked, UN organizations and NGO/IOs commit to the conduct of contextual, agency and programme specific risk analysis, which will establish common and individual risk profiles. While individual risk profiles will differ there may be opportunities for a common approach to SOPs between UN agencies and NGO/IOs which should be exploited, taking into consideration already existing standards, principles, and/or guidelines for example the UN MOSS (Minimum Operational Security Standards which are binding for the members of the UN system) and Interaction’s Security Planning Guidelines.</td>
<td></td>
</tr>
<tr>
<td><strong>6) Seeking Adherence to Common Humanitarian Ground Rules (CHGR)</strong></td>
<td>SLT recognizes that respect for common, locally developed ground rules for humanitarian action tailored for specific field locations enhances staff and operational security. CHGR seek to ensure that humanitarian assistance should not be instrumentalised by political or military agendas, should maintain its impartial character and be proportionate and based on needs only. The DO/NGO/IOs initiate discussion of development of CHGR applicable to local circumstances</td>
<td></td>
</tr>
</tbody>
</table>

---

3 Moreover, every effort should be directed to ensuring the issue of programme criticality is addressed from the start given the link between programme and security. As the recommendation is contextual, this recommendation applies as is to all three Stages.
SLT institutional arrangements – Means of propagating the revised SLT are addressed through the reinforced institutional arrangements, global and country level security training initiatives, and by piloting SLT in predetermined locations. To ensure buy-in from all constituents, the institutional home of SLT should remain the IASC, however the SLTTF identified the requirement for a permanent IASC SLT coordination resource to guide the implementation of the recommendations contained herein (in particular those that require long range investment such as reinforced risk management approach and security training initiatives), ensure momentum is maintained and that best practises are collected, analysed and disseminated in a manner similar to other IASC products. At the country level, there is an urgent requirement for dialogue on security matters at the professional level in the field, which should be addressed in the context of a local Security Working Group, comprised on UN and NGO security personnel, which would ensure the efficacy of joint security programmes.

SLT Information Management Approach - As with the other elements of the revision, the approach to implementation of recommendations towards information-based decision making has implications at global and local levels. The global commitment to information-based collaboration has never been stronger than it is at present, but there remain serious obstacles in the field demanding a concerted effort including training, advocacy, trust-building and field animation. While the staged approach described in the above table reinforces the mechanics of collaboration, there must be a strong commitment to overcome the longstanding issues of confidence, confidentiality and perhaps most important of all, recognition of the importance of the information sharing process. A common framework for incident analysis remains elusive but it is evident from initiatives in this direction that a common approach to security terminology is the most effective basis for collaboration in information sharing. To this end, the SLTTF endorses the DSS Security Threat Information (STI) framework (outline attached as an Annex) as the most viable option for delineating a common lexicon for security information and has initiated a preliminary survey of NGOs, which indicated a positive response to this recommendation.

Piloting and facilitating SLT - The identification and development of SLT implementation teams to facilitate SLT in selected pilot countries (CAP countries with multiple NGOs/UN agencies) was identified as a priority in this regard,. The SLT implementation teams, comprised of highly experienced UN and NGO security professionals, should be deployed on short term missions to pilot countries to establish SLT arrangements pending the development of in-country capacity, and should undertake periodic follow-up missions. As it stands, the preliminary list for piloting of the revised SLT Framework would include Afghanistan, DRC, Haiti, Chad, and Pakistan, as well as emerging crises in which the SLT model should be implemented from the onset of the crisis. Henceforth, the identification of areas for SLT implementation should be on the basis of consultation between members of the aforementioned IASC SLT coordination resource (paragraph 6, Executive Summary).

Security training - The security training element was most advanced prior to the formation of the SLTTF, as there was a long standing proposal for a joint UN and NGO security training CD-ROM or internet based application for operating in high risk environments. The SLTTF fully supports this initiative and will contribute to it realization, while at the same time working with DSS and INGO security training providers to ensure that the revised SLT, including the new security risk and
information management approach, are incorporated in all staff and security officer training platforms. The training programme should have a dual focus, to calibrate extant SLT initiatives in line with the revised approach and to initiate SLT arrangements in countries with little or no SLT activities, selected through a representational process.

SLT Funding Base - The recommendations of the SLTTF will require considerable donor support to be effective. While expertise is available, lack of resources has been the major impediment to SLT implementation. Surveys have shown that security is the least funded sector in the Consolidated Appeals (Annex II) and remains the most difficult subject to broach with member states hosting humanitarian operations. In light of these factors, a radical approach is required to revitalize the security regime for humanitarian operations. To this end, the SLTTF recommends, as others have, the establishment of a prorated (based on cost of operating not just cost of programme) approach to security in CAPs or other funding mechanisms to ensure availability of urgent security requirements. A portion of each contribution would be earmarked for security requirements contingent upon the type of crisis - i.e. in general terms open conflicts present more security challenges than natural disasters and so will require more funding to ensure an enabling security environment. The proposed SLTTF will work with the OCHA CAP unit and the IASMN to devise an appropriate formula for security requirements, and will provide models representing best practises with a target providing such guidance by the beginning of the CAP process for 2012.

As indicated in the attached Donor commissioned Report: Supporting security for humanitarian action: A review of critical issues for the humanitarian community, there has been a dearth of funding for security requirements and the situation is complicated by the approach of embedding security costs. The SLTTF Chair, on behalf of the SLTTF, has initiated a dialogue on Saving Lives Together with the Member State Donor groups, the Good Humanitarian Donorship Initiative based in Europe, and the Humanitarian Liaison Working group at UNNY, with the aim identifying, inter alia, means of widening the SLT donor base and developing a group of Member State “Friends of SLT” to ensure the necessary long term support. The issue of security is of growing concern to donors; however they are divided on how best to approach security requirements in the current operational environment. Against the background of the global economic downturn, development of a viable donor support base will require dedication and commitment. The SLTTF-recommended long-term SLT coordination resource in the IASC, should be tasked with donor liaison and the management mechanism for ensuring that SLT projects and funds benefit the broader humanitarian community and meet the mutually identified priorities of all SLT partners.