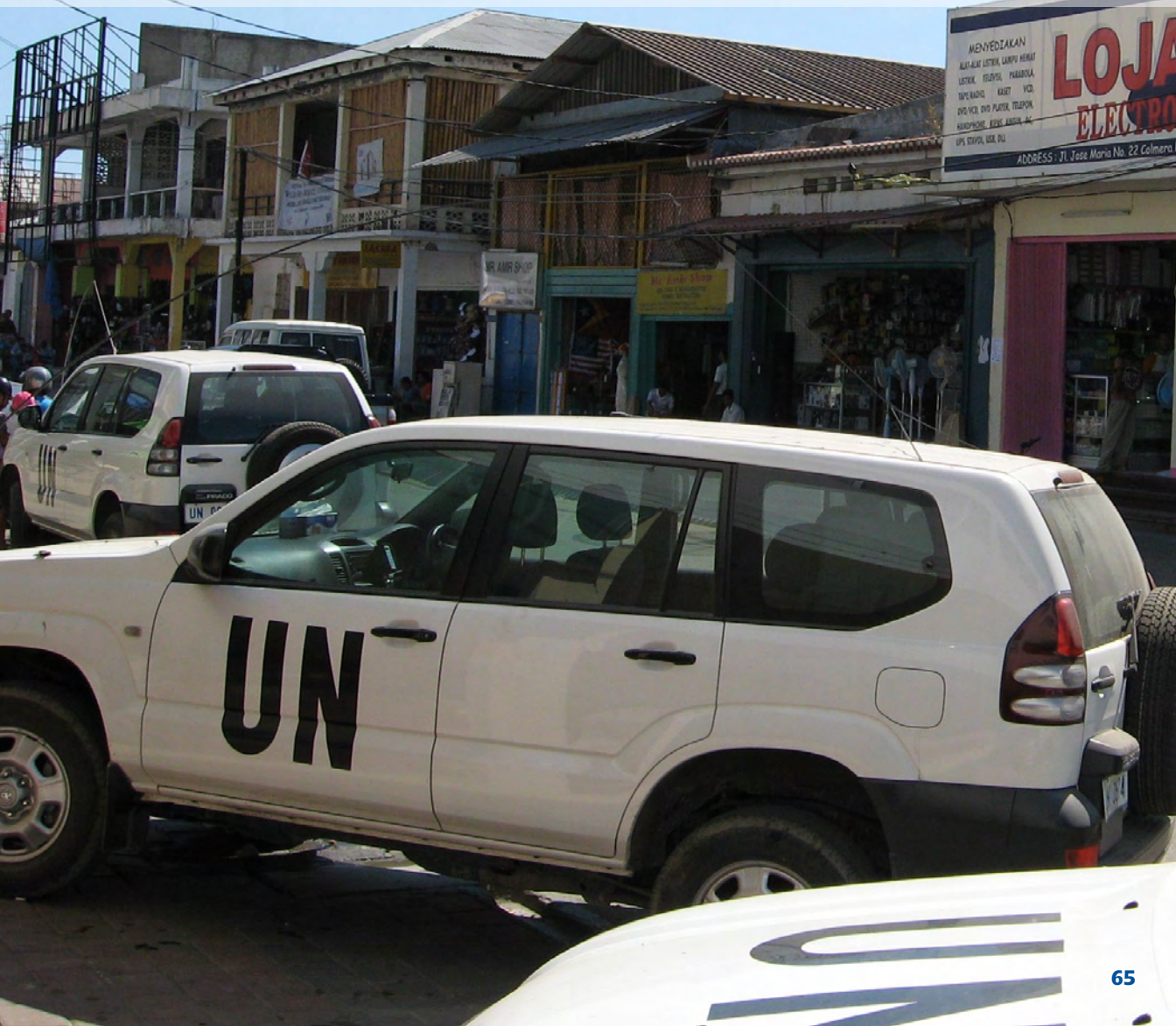
: CHAPTER 5 :

Field Security Plans



: NOTES :

Field Security Plans

Field security planning is the most critical business process CRS undertakes as part of its overall security management system. Field security planning is not a document, it is an ongoing process of 1) collecting and analyzing information about security in the operating environment, 2) adapting policies and procedures as the risk assessment changes, 3) knowing what to do if a security event does occur, and 4) practicing those responses so that they are more automatic. CRS applies a risk management approach to security by identifying, assessing and reducing risk to an *acceptable* level. The development and implementation of appropriate Standard Operating Procedures (SOPs) and Contingency Protocols are the means by which the organization reduces security risk. Once the security environment deteriorates to the point where CRS can no longer manage the levels of risk at an acceptable level, evacuation procedures may go into effect (for a short-term deterioration). Alternatively, withdrawal from high risk areas and full program closure are options that must be considered in a situation of long-term or chronic deterioration.

POLICY: Each field program must possess a written field security plan, updated annually at a minimum. This plan should cover issues related to all staff—international, national—and visitors. (POL-HRD-INT-0005)

Each field program and any sub-offices should possess a written field security plan with standard operating procedures covering everything from vehicle management to evacuation. The existence of field security plans facilitates staff/dependent, temporary duty (tdy) and visitor orientation and training with regard to standard operating procedures and rules to be respected to reduce the security risks of his/her mission.

TIPS - Field Security Plans

1. Don't rely on an external TDY to write your Field Security Plan (FSP).
2. Do invite someone to facilitate a participatory FSP review workshop, if there is no one with this capacity internally.
3. Do include as many national staff and international staff as possible in the FSP development process, representing all "levels" of the organization.
4. Do follow up with staff training where relevant—practice the protocols.
5. Do update the full assessment at least annually; consider using the Rapid Risk Assessment matrix for quick updates to SOPs in volatile environments.
6. Do use the Security Levels document as a management tool, as the basic rules for a "normal" situation might not necessarily be the same as for a "crisis" situation.
7. Do include a "Last Updated: xx/xx/xxxx" header or footer to indicate the date the plan was last updated and approved.
8. Do have the Field Security Plan reviewed and approved at the regional level prior to uploading to the CRS Safety and Security Portal.

The *CRS Field Security Plan* documents the complete Threat, Vulnerability and Risk Assessment process, as well as the operative procedures and protocols that are generated from that assessment. Risk assessment is a continuous process, and must be updated at a minimum annually. Depending on the nature of the security environment, a more frequent update may be appropriate. Staff in each country program should have read and understand the entire field security plan for context; the appendix documents are those which should be kept on hand and used for implementation.

The CRS Field Security Plan Format
I. Introduction: Purpose of the Plan.
II. Operating Environment.
III. Threat, Vulnerability, and Risk Assessment.

Appendices
- Standard Operating Procedures (SOPs).
- Contingency protocols.
- Security Levels—Triggers and SOPs.
- Constant Companion.
- Communications Tree.
- Relevant Maps.
- Rapid Risk Assessment (RRA) matrix (recommended for volatile environments, for use by CR and Security Officer only).
- Evacuation Plan (for CR, Security Officer, and need to know persons only).

I. Introduction: Purpose of the Plan (maximum 1 page)
The introduction to the Field Security Plan outlines for all staff and families the practicalities of their responsibility to be familiar with the plan, and specifically who in the country program is responsible for making security management decisions based on the plan.


Example Introduction from CRS/Egypt:

Purpose of this Security Plan
CRS provides this security plan to all staff and agency guests (including dependent family members of international staff) residing, working in, or visiting this country program. The aim of this security plan is to inform all staff / guests of location-specific security rules and procedures that apply to or are in effect for CRS in Egypt. It does not repeat generic security rules or procedures that are common to most operations in insecure locations. For those, please refer to **CRS Staff Security and Safety Guidelines**.

Every member of the CRS country program team, staff and non staff guests has a responsibility to promote security, and is required to follow all rules and procedures in this security plan. Failure to do so could endanger life, and is a disciplinary offense. This security plan is designed to keep you and your colleagues safe, and to enable CRS' work to run smoothly.

The person in charge of CRS Egypt security is Luc Picard, Country Representative (CR) for CRS Egypt. The national Security Focal Point person is Ashraf Rammeya, Operations Manager. This security plan will be updated as often as necessary—annually at a minimum. All staff is encouraged to contribute updates as the need arises through the persons named above.

CRS EME Regional Security Officer, Todd Holmes will provide advisory guidance and recommendations related to security situations.

All staff are required to read this as part of their orientation and sign **Annex 2** of this local field security plan and retain a copy with critical information. If you have any questions about it, or suggestions for improving it, please inform your manager or the Security Focal Point as soon

as possible. For visitors and new staff coming to the country a shorter **Visitor Security and Safety Briefing** is available on the security portal.

You should have a copy of the CRS Staff Security and Safety Guidelines and be familiar with all agency policies related to security matters—ask the SFP for further information. Agency security manuals, policies, and field security plans as well as other documents can be accessed on the **CRS Security Portal** through the agency intranet. Please take some time to visit this resource.

II. Operating Environment (maximum 2 pages)

This section outlines relevant information from the historical, political, economic, geographic and perhaps public health context that have safety and security implications. CRS history of operations in the country might also be summarized, particularly if that history includes information that would assist the reader to understand the nature of CRS' unique vulnerability to certain security threats in the country.

III. Threat, Vulnerability And Risk Assessments (suggested 1-3 pages)

Risk Assessment is an ongoing process and is the foundation on which all other field security plan documents are based. The full process of updating the documented analysis should take place at a minimum annually. For environments where conditions change rapidly, consider using a matrix version of the Threat, Vulnerability and Risk Assessment to summarize key information and any new security measures to be implemented as a response to new or changing risks. (See the Risk Assessment section for more information on the Rapid Risk Assessment matrix (RRA).

The format for presenting the summary results of the Threat, Vulnerability and Risk Assessment should involve a simple listing of identified threats, organized by office location/region to the extent that the security environment differs and requires distinct operating procedures. For each threat, provide some analysis as to patterns, trends, and factors of vulnerability of CRS staff, assets, and programming to the threat.

Example Risk Assessment from CRS/DRC-Kinshasa:

A) Urban Crime/Banditry

The level of crime in Kinshasa has been low for an African city of its size. Break-ins, car-jacking and muggings are rare. It should be noted that there have been upsurges of crime in the past, however, at times when military discipline has broken down. The level of crime in Congo/Brazzaville is similarly low. It is however to be noted that law enforcement authorities usually respond to crimes slowly, if at all when they happen, (there is a lack of resources and commitment) and provide little or no investigative support to victims. Crime is also committed by or with complicity of persons in police/military uniforms.

B) Abduction and Harassment of NGO Personnel/Operations

Direct serious threats against NGOs have been very rare in Kinshasa and other large cities in the DRC. They are mostly limited to isolated areas in the interior of the country with humanitarians in Ituri and isolated areas of the Kivus being at most risk. Reported incidents of vehicle requisitioning, harassment, looting of goods and abduction of NGO and UN Agency personnel at the hands of the Congolese military and security forces, militias and ex-combatants in isolated areas, demonstrate the vulnerability of aid agencies. Few incidents appear to be politically motivated and are mostly related to urgent resource needs of these

different armed groups. Movements of CRS staff or material to those isolated areas should be carefully monitored in order to prevent those risks.

C) Indirect Threats: Public Demonstrations/Looting

The primary security concern of CRS/Congo staff is the indirect threat of being caught up accidentally in public/ political demonstrations, fighting and/or looting by armed groups. Some formerly rebel-occupied areas of Eastern Congo, which are still scenes of isolated clashes between armed groups, represent a high level of indirect threat as well. In addition some formerly rebel-held towns in the country (e.g. Bukavu, Goma, Bunia, etc.) have experienced attacks, violent demonstrations, or inter-communal violence over the past six years. Most of these events occur without warning, though the great majority have been concentrated in several chronically unstable areas including Ituri and Northern Katanga.

In contrast, the level of indirect threats in Kinshasa and formerly government-controlled areas are currently very low. Nevertheless the city, and indeed the entire country, has a recent history of widespread looting lead by the military. There is always a small possibility that unforeseen political or economic events could trigger similar chaos in the future.

D) Vehicle Accidents

The number of fatalities caused by vehicle accidents is high in the DRC with rural roads being the most dangerous. Roads, when existent at all, are in very bad conditions and characterized by poor surface, mud, potholes, lack of road signs, very poor (almost inexistent) road lighting etc.

Common causes of accidents on Congolese roads include:

- Ignorance and/or lack of compliance with road signs and road regulations.
- Aggressive driving of official vehicles (e.g. presidential motorcade).
- Reckless driving of most vehicle users (e.g., failure to signal, use of high beams, sudden stops).
- Reckless use of the road by pedestrians and cyclists.
- People causing an accident on purpose to extort money from drivers.
- Arbitrary operation of traffic lights, not respected by most road users.
- Poor condition of most vehicles.
- Overload of vehicle.
- Driver fatigue.
- Bad road conditions and infrastructure.
- Driving under the influence of alcohol, or drugs.
- Lack of concentration while driving (common usage of a phone/radio or chatting).

E) Police Harassment

Road traffic harassment is the most common sort of Police harassment in Kinshasa where crowded intersections and snarled traffic routes are common. Due to the irregularity of the payment of local police/military salaries and the presence of desperate traffic officers, such individuals are exploiting situations where there is blocked traffic to harass motorists. Avoiding these situations is not always possible; Confrontation with these officials should be avoided. Even if handled properly, these confrontations have the potential to escalate.

Some Definitions:
Risk = Threat x Vulnerability

Threat
A danger or hazard in your operating environment; any possible occurrence that may cause injury to CRS personnel, loss or damage to CRS property, or program delays or suspension. Generally, all organizations face the same threat environment in any given location.

Vulnerability
The degree of the *impact* that any given threat event would have on CRS personnel, assets, or programs. The *likelihood* that CRS personnel, assets, or programs will experience any given threat event. There are many contributing factors that affect the level of vulnerability of CRS personnel and assets are to any given safety and security threat.

Factors such as the following mean that not all NGOs operating in the same operating environment will be equally vulnerable or exposed to the same safety and security threats:

- CRS identity.
- location of NGO staff and property.
- exposure of NGO personnel and property.
- value of NGO property.
- impact of NGO programs.
- adoption of appropriate security measures.
- compliance of staff with security measures.
- staff interpersonal skills.
- image of staff and programs.

Risk = Threat x Vulnerability
Risk is the potential for negative consequences to CRS staff, assets, and programs based on a combined assessment of 1) the likelihood of a threat event; and 2) the severity of impact on the organization should a threat event occur.

The Threat, Vulnerability and Risk Assessment process forms the basis for all other Field Security Plan documents. Conducting a safety and security Risk Assessment involves the following steps:

A. Threat Assessment: Information is collected on current safety and security threats in the operating environment.

B. Vulnerability Assessment: Information about threats is analyzed through the lens of CRS' program profile in-country to understand how CRS might be more or less vulnerable to the various threats.

C. Risk Assessment: A risk rating (from Negligible to Critical) is assigned to each type of threat based on the analysis of how likely a given security event could occur to CRS, and how severe the impact on CRS operations should a given security event occur. The aggregate risk assessment should inform the overall Security Level in place for the relevant CRS location.

A. Threat Assessment

The threat assessment exercise should begin with an overall understanding of the country context and its history—understanding for example the country's history of civil conflict, political parties and their affiliations with international, non-state, private sector, etc. actors may be important to finely hone the assessment of potential threats to NGOs, humanitarian actors, development agendas in certain locations of the country, how a U.S. and Catholic organization might be perceived and accepted (or not), etc.

There are three main types of threats: Direct, Indirect, and Crime/banditry.

Direct Threats

Include actions taken by a belligerent (usually to aid in a political or military effort) for which NGOs are the intended target (such as robbing a food convoy).

Indirect Threats

Include for example actions taken by a belligerent for which the local population or other belligerents are the intended target but NGOs are unintentionally affected, such as NGOs getting caught in cross-fire or hitting a land mine on the road. Other examples include demonstrations/civil unrest and threats from traffic accidents.

Crime/Banditry Threats

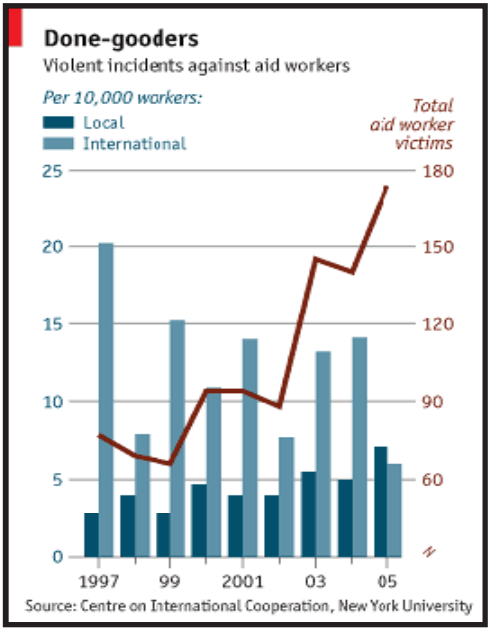
Include everything from pick-pocketing and other types of theft to harassment, illegal detention, carjacking (for theft), kidnapping (for ransom), to sexual assault.

To conduct a threat assessment, you will need to gather information and conduct interviews in order to identify the threats you may face by implementing a program in a certain area. Limit the assessment to your zone of operation. For example: a threat of attacks on a specific road in the north of the country may not affect your operation when you only work in the south.

Begin By Conducting Interviews

Careful, structured interviews provide broad information on the threats others have faced and provide a frame of reference for focusing other assessment techniques.

- Suggested interviewees include other NGOs, local partners, UN agencies, and the ICRC as CRS may face similar threats as these organizations.
- To develop a more comprehensive picture of the operating environment, interviews should be conducted also with people such as transporters, traders, journalists, church representatives, missionaries and other religious leaders and workers who may be the only persons to travel to some remote areas.
- In addition to all of the above, it may also help to interview local authorities, military and police. However it is extremely important when speaking to these last actors to always



focus your questions on humanitarian activities to avoid any misinterpretation of your intentions For example: rather than to ask about specific combat activity in a particular area to inquire if there is enough safety for CRS to travel and implement a program in that area.

It is also important to evaluate the accuracy of the information provided:
- Have you received information that is contradictory?
- Does the interviewee have direct or indirect knowledge of the information?
- Has information he/she has reported in the past been reliable?

For each known type of threat, it is helpful to prepare a worksheet for the interview which focuses on key questions that can be answered by those interviewed. Include issues such as location, types, situation, and likely cause of threats. For example, if there is a threat of car-jacking, it is important to know in which area it is likely to happen (A specific area? A specific road? Anywhere?). It is important to ask when car-jackings are most likely to occur (During the day? Evening? Late in the night? Early in the morning? Anytime?). How do most car-jackings occur (When reaching your vehicle? When stopped in front of your gate? At the traffic lights? Ambushed or chased by other vehicles?). And what vehicles are most targeted (4x4s? Executive sedans? Family sedans? Pick-up trucks? Any type?).

Look For Written Data
- Incident/situation reports from CRS and other NGOs, UN agencies, ICRC, OSAC, NGO security coordination mechanisms (e.g. ANSO in Afghanistan), local police, private security information services, etc.
- IRIN reports are usually received by CRS program where they have email facilities and inform on threats and security incidents faced by NGOs in the country.
- Explore media resources; in big cities the local press/radio often report on crime/ banditry incidents.
- On the Internet (various humanitarian agencies' sites, press releases, etc.) www.ReliefWeb.int

Best Practice

CRS staff conduct an (at a minimum) annual review and analysis of safety and security incidents, at the country program and regional levels, as one of many sources of input into the ongoing risk assessment process. Such regular analysis promotes improved understanding of which kinds of safety and security incidents CRS staff in a given context are most vulnerable to, and informs organized training priorities as well as investment decisions. An example of a regional summary report on safety and security incidents is included in the Appendices section of these guidelines.

Identify Specific Patterns And Trends

Examination of quantitative information on past security incidents helps to identify the most common features of security incidents (patterns) and changes in patterns over time (trends). Pattern/trend analysis may yield sufficiently reliable and specific information on threats (such as what roads are mined) on which to base security measures. To identify patterns and trends, data should be compiled on past incidents (date/ time, location, type, situation, and likely cause). As with interviews, other NGOs are often a good source of data.

To analyze the information, clusters of incidents should be identified (highest likelihood) by each factor, such as carjackings on a specific road. If you are concerned about indirect threats

(being caught in the crossfire) because the conflict has no clear battle lines, then patterns and trends related to the conflict that could indicate areas of dangerous activity (skirmishes, ambushes and massacres) should be identified.

Factors to consider when tracking patterns and trends apart from the specific threat types include:

- Time of day.
- Locations/routes.
- Number of perpetrators.
- Type of car/other object (i.e. radios) preferred by perpetrators.
- Weapons used (or not).
- Motive.
- Mode of operation (MO).

B. Vulnerability Assessment

Not all NGOs are equally vulnerable to the same threat environment. Vulnerability for CRS is the degree to which CRS staff and assets are more or less exposed to existing safety and security threats. Vulnerability assessments highlight CRS' susceptibility to various risk factors, for example examining how staff behavior or staff composition affects security. Although CRS staff cannot change the threat environment, they can influence staff behavior and programming, both of which profoundly affect CRS' vulnerability to threats.

Understanding CRS' specific history and profile in the country, (e.g. the quality of relationships with partners, host government, local authorities, non-state actors, the communities' perception of CRS, where we have offices, how many staff are employed, from which ethnicities and nationalities, is CRS involved in distribution programs, cash management procedures, etc.) all factor into our understanding of how exposed we are to a given security threat.

Vulnerability Factors:

- Location.
- Exposure of Staff/Property.
- Value of Property/Commodities.
- Impact of Programs.
- Adoption of appropriate safety and security measures.
- Compliance with Safety and Security Protocols.
- Staff interpersonal skills.
- Image of staff and programs.

Eight basic factors affect CRS vulnerability, but their applicability may differ depending on the cause of the threat CRS is facing (i.e., crime/banditry, direct threats, or indirect threats). Some of these factors affect CRS' vulnerability in all three situations, such as the location of CRS staff and property. Other factors have an impact only in certain types of situations. The value of CRS property, for example, matters when faced with a crime/banditry threat, but not with an indirect one (e.g., getting caught in the crossfire, artillery barrage, or mined areas).

1. Location

In an area or country in which threats vary significantly, CRS' vulnerability may differ from that of other NGOs due to the specific locations of CRS staff and property. The location factor applies to all three causes of threats.

2. Exposure of Staff and Property

CRS' vulnerability is partially dependent on its exposure or the extent to which CRS staff and property are in dangerous locations and/or unprotected. This factor varies by cause of threat:

- If the threat is *indirect* (getting caught in the crossfire), then reducing exposure will probably help.
- If the threat is *crime/banditry,* reducing exposure may help if those threatening CRS threaten everyone (the local population and expatriates alike) and/or protective measures are effective (which may not be the case against well-armed criminals or bandits).
- If the threat is being directly *targeted* by belligerents, some protective measures may make CRS less vulnerable, with three possible exceptions:
  a. Protective measures may be ineffective against well-armed belligerents determined to threaten you, as seen in Rwanda and Chechnya.
  b. Depending on the situation, protective measures that decrease CRS interaction with the population may alienate CRS staff more from them, and increase vulnerability (as discussed in earlier sections on agency image and acceptance).
  c. Depending on the situation, protective measures that associate CRS with one side in a conflict (e.g. use of military escorts) could increase CRS vulnerability.

3. Value Of Property

NGOs with more valuable property may be more vulnerable. NGOs in general have valuable property (cash, equipment, vehicles, personal property, and relief aid). In any situation, these items are a potential target of criminals. If a CRS field program is operating in a conflict zone, belligerents may target CRS property to support their military efforts. This factor applies primarily to crime/ banditry and direct threats (targeted by belligerents).

For example:

- Stolen cash can be used to purchase military equipment and supplies (e.g., weapons, ammunition, vehicles, fuel, radios, food).
- Some NGO property can be sold or bartered (e.g. vehicles, radios, medicine, valuable foodstuffs); and, some NGO property has military value to combatants (e.g., four-wheel drive vehicles, radios, fuel).

4. Impact of Programs

NGOs whose programs have an impact on different groups or (even minimally) benefit one of the belligerents in a conflict may be more vulnerable than others. Although the impact of aid on conflict situations may sometimes be overstated, there is no doubt that most aid programs benefit some groups more than others. *Being aware of this helps to better understand your vulnerability.*

The most commonly cited situation is when belligerents use roadblocks and ambushes to divert aid and provide it to their military forces and the population supporting them. As described in the Threat Assessment section, even if they do not divert CRS programs, they may threaten CRS if CRS is *perceived* as supporting their opponents. This may be the case with food aid provided to vulnerable, civilian populations in areas occupied by one of the belligerents because of the ways in which it may affect military efforts. This factor applies to direct threats (targeted by belligerents).

5. Adoption of Appropriate Security Measures

Organizations that adopt appropriate security measures are less vulnerable than those that do

not. Security policies and procedures should reflect a mix of strategies (acceptance, proctection, deterrence) that responds both to the nature of the threats in a given operating environment, as well as reflecting CRS' identity. The participation of national staff and local partners in the definition of appropriate security measures also helps to ensure their effectiveness vis-a-vis the local cultural context.

6. Compliance with Security Measures

Even assuming a CRS field program adopts appropriate security measures, the level of vulnerability is still dependent upon whether the staff consistently complies with them. NGOs usually adopt a wide variety of measures, from broad policy (such as prohibiting soldiers or armed persons from riding in vehicles) to minute procedures (how to call for help using a radio). Assuming these measures are appropriate, CRS staff is more vulnerable if they do not comply with the measures. This factor applies to all three causes of threats.

7. Staff Interpersonal Skills

The interpersonal skills of CRS staff can affect vulnerability by helping to avoid incidents and mitigate their impact if they occur. As described in the sections related to individual behavior, such skills affect security in important ways.

When confronted with an incident (e.g., roadblock, angry mob), skills and behavior can either escalate the incident or de-escalate it, depending in part on an individual's skills in dealing with a stressful situation and negotiating effectively.

Second, individual skills and behavior with regard to team-building and developing relationships can help prevent incidents from occurring (through sharing information and ensuring buy-in to security measures) and can mitigate the impact of incidents (through mutual support of team members). From the perspective of reacting to incidents, interpersonal skills are most important when facing crime/banditry and direct threats (by belligerents, except when the types of incidents are those not allowing for any interpersonal interaction (e.g., ambushes, bombing, some assaults).

CRS CHAD: In *Chad*, a friendly relationship between one CRS staff person and their neighbors helped to prevent the CRS residence from being looted when the CRS team was evacuated.

CRS Afghanistan: In *Afghanistan*, friendly relationships between CRS and neighboring families forms an important part of the team's contingency plan for the potential threat of home/compound invasion by armed belligerents. Ladders are pre-positioned to assist staff escape over neighboring walls and neighbors have agreed to assist CRS staff to take refuge in their compounds if the CRS compound is attacked.

8. Image Of Staff And Programs

Vulnerability is partially dependent on the image which CRS projects. As discussed earlier in the guidelines, every NGO has an "image" which informs the perceptions of the local population, authorities, and belligerents toward the NGO's staff and programs. This image matters. What CRS staff say and do, their appearance, what mix of ethnicities/nationalities they are, and the

shape and impact of CRS programs influences the opinions of the local population: Will they accept CRS' presence and roles, or be resentful toward the agency?

While image may not be the sole cause of significant security incidents, acceptance or resentment of CRS' staff and programs can influence security in important ways:

- It increases or decreases the predisposition of criminals and belligerents to target CRS.
- It makes the local population more or less likely to help ensure that CRS staff do not face security incidents (such as by extending societal constraints on criminal activities to CRS staff and property, and forewarning CRS of danger)
- It makes the local population more or less likely to help CRS staff when they are actually confronted with security incidents (such as by helping to recover stolen property).

Special Risk/Vulnerability Considerations

Apart from the eight basic risk factors that affect vulnerability, outlined above, other context-specific risk factors should be explored, and may result in differentiated security measures related to the unique vulnerabilities of:

- Specific program areas.
- Gender Considerations.
- National vs. International staff.

Program Areas

CRS staff faces particular risks when working in some program areas more, or differently, than others. The key to good security management is a sound in-depth analysis of the risks faced by staff as an integral part of the program assessment and design process.

Examples:

- **Emergency Response:** in the case of natural disasters where the water infrastructure has been destroyed there is an increased risk of exposure to waterborne illnesses that presents threats to the CRS response team, even as it threatens beneficiaries. Complex emergencies and civil conflict present more convoluted safety and security challenges as there may be a mix of direct/indirect and crime/banditry threats at play. The image of the organization, in terms of how we are viewed by the various parties to the conflict as well as communities affected by the conflict, will affect both our capacity to work effectively and to do so safely. CRS should carefully consider the mix of staff hired to work in certain locations—different contexts will suggest which nationalities, ethnicities, religious orientations, genders, etc. will be more or less effective. CRS management must balance considerations of access (employing staff with positive and strong connections/relationships to local power structures) and impartiality (not employing too many staff apparently aligned with one "side" of the conflict more than another). Where there are international military actors present, overtly or covertly active in the conflict, CRS management may consider avoiding employment of certain nationalities that may face greater risk of being perceived as aligned with or connected to the international military agenda. Programming responding to internally displaced persons (IDPs) and refugees requires some additional analysis focused on how program design might reduce risks for displaced populations and for CRS staff attempting to reach them. In particular some protection concerns might include: how an IDP camp is designed; how basic needs of IDPs are resolved (i.e. firewood collection, food/non-food item distributions); how CRS and displaced populations benefit (or don't) from armed protection services, among others. CRS might intentionally seek to serve populations from both "sides" of a conflict. This

can help ensure that programs benefit both displaced persons and host communities (in order to safeguard the image of the agency as impartial and neutral) but also to mitigate tensions within communities, to further ensure our security as well as the people we serve.

- **Advocacy:** CRS, as a general rule, does not advocate for public policy changes overseas, but we do support local partners who do so. When local partners undertake advocacy projects that take aim at issues that implicate government officials, or other local power structures, at times those (formal and informal) power structures strike back. For example, projects that work on issues of corruption and transparency around extractive industries have resulted in the imprisonment of partner staff. Partners who have conducted advocacy on behalf of migrant populations have experienced break-ins and ransacking of their offices. It is important for CRS and partners to dialogue openly about the risks such programming implies, and how CRS might support partners to help them face or mitigate security-related contingencies. Potential special threats to consider here might include: office theft, harassment, or detention of staff by government authorities. Special consideration of the need to maintain information as confidential and secured may be required, in addition to thinking through contingency and business continuity procedures in case the office is looted or key staff are detained.

Risks Faced By Women Versus Men

Women face unique, gender-based threats in crisis situations: the danger of sexual assault. Increasingly, rape and other sexual threats are used in the strategies of war. However, the differences between the risks that men and women face in the field are frequently subject to exaggeration. This is particularly dangerous for men, who may be tempted to see themselves as invincible in contexts in which their vulnerability is actually at a level very similar to that of women. Therefore, gender-neutral security policies and procedures should be strongly encouraged overall. For example, a "buddy system" or curfew policy should be encouraged for men as well as women rather than one gender alone.

CRS field offices should make a concerted effort to develop an understanding of the culture in which they are operating and the threats unique to women in that context at the same time as empowering women to carry out their work effectively. Female and male personnel alike must think critically about the dangers associated with their context and then feel empowered to make sound judgment calls about what type of behavior to adopt at which times.

One additional resource on risks specific to women is "UNDSS[1] Security Guidelines for Women": http://www.searo.who.int/LinkFiles/Field_Security_Services_Sec_Guidelines.pdf.

CRS Afghanistan operates in a context that is extremely challenging for female staff—from the perspective of recruitment (norms related to women's roles) as well as travel to project sites. This same local culture governing appropriate interactions between men and women places a premium on having female staff who can reach out to female beneficiaries in a more open and culturally appropriate way. As a partial response to this challenge, CRS Afghanistan has tried in some cases to employ married couples, so that the husband can accompany his wife when field visits to communities are required. This approach supports local women to pursue their desired careers, while respecting the local culture, and also enables CRS Afghanistan to more effectively implement programming by reaching out to female as well as male members of beneficiary households.

1 United Nations Department of Safety and Security (UNDSS)

Risks Faced By National Versus International Staff[2]

There are two major kinds of risk for CRS staff in the field: external and internal risks. Many security policies such as housing selection, curfews or evacuation apply only to international staff, reflecting the additional risks incurred by staff living away from their "home" culture and support networks, as well as the fact that internationals reside (and assume security risk) in foreign locations due solely to their CRS employment conditions. However, just as there are risks for international staff, there are special risks unique to CRS national staff. In fact, a recent study found that national staff comprise 78% of all NGO staff victims of violent security incidents, and that this statistic is growing while the incidence rate for international victims of violence is stable or declining.[3] In part this statistic may be due to the fact that they are simply more absolute numbers of national staff than international staff working in NGO field offices. It may also reflect the care with which NGOs have traditionally selected and protected international staff housing and transportation situations, as opposed to national staff which live in their own homes and largely make their way to work and home again by their own means, even if we would strongly discourage an international from using public transportation, for example. Whatever the explanation, international field program and HQ staff should be sensitive to the risks faced by national staff, and work together with national staff to analyze the risks and develop smart yet practical standard operating procedures that take into account the unique exposure of national staff due to the fact that they work for CRS. These might be the "internal" risks more than the "external" ones, to which nationals would be exposed whether or not they worked for CRS.

External risks are directly linked to the operating environment, such as:

- Shelling, grenades, shooting (war context).
- Looting, burglary, crime (anarchy context).
- Disease (linked to tropical country environments and water/sanitation conditions).
- Shooting, violent demonstrations and protests (civil unrest).
- Car accidents (dangerous traffic), poorly maintained vehicles, few traffic laws.
- Natural disaster (volcano, earthquake, flooding).

Internal risks directly linked to professional actions within CRS include:

- Handling large amounts of cash to pay salaries or to make purchases.
- Staff equipped with visible radio handsets and other technical equipment.
- Transporting commodities.
- Driving a CRS vehicle.

Note: Any driver of a CRS vehicle assumes additional personal risk whenever getting behind the wheel. In case of an accident, particularly if it results in injury or death, the driver can be subject to incarceration, mob justice, or simply a large financial liability (especially in the case of international staff using cars for personal use).

CRS Kenya's experience with ethnic-based post-electoral violence in the early months of 2008, is an example of when "external" risks can impact national staff more than international staff. In this situation, CRS Kenya prioritized international staff over nationals for deployment to the most volatile areas during the emergency response period. When national

2 For additional reference material, see the Appendices for a copy of the InterAction document, "The Security of National Staff: Essential Steps."

3 Abby Stoddard, Adele Harmer, and Katherine Haver, "Providing Aid in Insecure Environments: Trends in Policy and Operations," CIC Briefing Paper, New York University in collaboration with the Humanitarian Policy Group, Overseas Development Institute: December 2006.

staff did deploy, the ethnicity of the person was a primary determining factor in deciding who would go to which region, as different ethnicities were threatened in different areas of the country.

For the purposes of these guidelines, four kinds of risk that may impact national staff to an equal or greater extent than international staff have been identified for consideration.

1. Risks Linked To The Context
National staff directly experience the same external risks related to the operating context as do international staff. These risks, however, are compounded for national staff due to the impact of the same events (shelling, shooting, increased armed robbery, etc.) on their network of family and friends. Standard operating procedures should be developed by all field programs to address the professional risks related to CRS work in a specific context.

Each individual staff member is responsible for respecting the SOPs in order to minimize professional risks. Yet, personal risks can be as much of a threat to security as professional risks. CRS staff should be aware that inappropriate personal behavior is the most common cause of insecurity for humanitarian aid organizations. Chaotic situations can sometimes make it seem as if anything is possible and anything is permissible, especially when local legal institutions and law enforcement are weakened or non-existent.

2. Risks Linked To Employment
Employment with a humanitarian aid organization distinguishes national staff from the rest of the local population. At times, the perceived power national staff has over much desired aid resources can lead to significant pressure (e.g. pressure on the warehouse keeper to look the other way as a few bags of corn go out the back door). In the most extreme cases of armed conflict, hiring a member of a particular clan/tribe/ethnicity/religion can skew the general public's perception of the organization, and put the employee in physical jeopardy if placed in particular situations. In-depth knowledge, by management, of the local context is essential to manage staff security.

3. Risks Connected To CRS Activities
In some contexts CRS' strategy and program activities are not understood and/or accepted by the general population or a particular group. Even if international staff is seen in a favorable or neutral light because they are foreigners, national staff may be perceived as privileged or even as traitorous to a cause.

4. Risks Linked To Professional Tasks
National staff may also face risks that are even more directly related to their professional responsibilities than international staff. For example, guards may be subject to attack, finance staff may be exposed to robbery attempts and a driver crossing a checkpoint with food may be seriously harassed. Again, well-analyzed, designed and observed SOPs for these situations will minimize risk.

C. Risk Assessment
The combination of the threat and vulnerability assessments (risk = threat x vulnerability) helps to identify the most likely types of threats CRS will face, as well as those which would have the greatest negative impact on personnel, assets, and operations. This analysis, or risk assessment, leads to the identification of the most appropriate security measures that respond to those specific threats.

Each threat can be categorized as a Negligible, Low, Medium, High or Critical Risk according to definitions provided within the Risk Rating Matrix below. Determining factors for how severe the risk include: 1) How likely a security event of this nature is to occur; and 2) the severity of impact on personnel (injuries, death), assets (value of loss), and programming (no disruption to complete suspension).[4]

Impact → / RISK / Likelihood ↓	NEGLIGIBLE No serious injuries. Minimal loss or damage to assets. No delays to programs. (1)	MINOR Minor injuries. Some loss or damage to assets. Some delays to programs. (2)	MODERATE Non-life threatening injury. High stress. Loss or damage to assets. Some program delays and disruptions (3)	SEVERE Serious injury. Major destruction of assets. Severe disruption to programs (4)	CRITICAL Death or severe injury. Complete destruction or total loss of assets. Loss of programs and projects (5)
Certain/ Imminent (5)	Low	Medium	High	Critical	Critical
Very Likely (4)	Low	Medium	High	High	Critical
Likely (3)	Negligible	Low	Medium	High	High
Moderately Likely (2)	Negligible	Low	Low	Medium	Medium
Unlikely (1)	Nil	Negligible	Negligible	Low	Low

For example, if the threat of banditry is such that the likelihood of a CRS vehicle being stopped by armed men and assaulted on the way to a project site is determined to be "likely," and the impact of such an assault could result in serious injury (as the bandits carry weapons) and there is also a possibly for the loss of the vehicle as well ("severe impact"), then there is a corresponding "High" risk rating assigned to the threat of banditry. In this particular country program, a high risk rating may be above our acceptable risk threshold. CRS would want to more closely analyze the banditry threat in our operational area, and try to develop some standard operating procedures (SOPs) that would reduce the risk—either by decreasing the likelihood of this threat occurring or by decreasing the impact to CRS of a threat event.

APPENDICES

A. Standard Operating Procedures (SOPs) should flow from the risk assessment and are generally defined as those procedures which are followed prior to an incident. SOPs are measures that reduce the risk to CRS staff and assets—either by reducing the likelihood of occurrence, or the impact should it occur. Full participation by national and international staff in the development of SOPs achieves two objectives: 1) ensures that SOPs are the most

4 The Risk Rating Matrix and standard definitions of likelihood and impact levels form part of the United Nations Department of Safety and Security (UNDSS) approach to Security Risk Management and was published on June 24, 2004.

appropriate to effectively and practically reduce the risk factors associated with a given threat in a given context; and 2) facilitates higher levels of compliance with determined SOPs by the same staff who developed them in the first place. Communicating frequently with staff about the nature of the risk environment, and how SOPs are linked to the threats prevalent in the operating environment, will aid in sustaining awareness of and compliance with security protocols.

Identification of prevention and mitigation measures asks, what are the policies, protocols, or procedures that require strengthening to more effectively reduce CRS' exposure to safety and security threats?

The SOP document will include the following categories of procedures:

1. General Security Rules (or "Golden Rules")
General Security Rules are general "Do's" and "Don'ts" that apply to all individuals and provide guidance for personal security awareness and behaviors that will promote personal safety and security in the local context. These "Golden Rules" can be everything from what to wear and how to greet people in the local context, to the more generalizable behaviors such as "be aware of your surroundings" and "always wear your seatbelt."

2. Staff Movement
- Standard operating procedures—travel authorization, route verification, general travel policies (e.g. no travel after dark, use of logo or not).
- Movement in town.
- Movement outside of town and in rural areas.
- Maps of any no-go roads/zones.
- Cautions on approaching checkpoints.
- Response in case of car accident.
- Radio procedures for field trips.
- Kit for vehicle (basic first aid and spare parts).
- Convoy procedures.

3. Radio And Other Communications
- Rules for using radios in crisis situations.
- CRS radio checks and protocols.
- Radio protocol and channels for other organizations.
- Important frequencies and call signs.
- Other communications policies.

4. Management Of Offices And Residences
- Management of personnel concerned with security (job description for guards).
- Maintain a list of emergency stocks per location.
- Policy regarding safe rooms, if relevant.
- Fire safety.
- Office access control procedures.
- Cash/confidential documents management.

5. Staff Health
- Health risks and how to prevent them.
- Vaccinations required.

- List of health services available locally.
- Pandemic procedures (if relevant).

Following the example of the high risk of banditry from above, some procedures that might be re-considered in this case:

- CRS logo and type of vehicle: Does the CRS logo and 4 x 4 vehicle attract unwanted attention? Would it reduce CRS appeal to bandits if we were to remove the logo, or use an older, well used (rented) vehicle for traveling to certain destinations? Is the risk associated with the breakdown of such a vehicle higher than the risk of driving with a logo and 4x4 or sedan? Does the local partner have higher acceptance along this route and therefore traveling exclusively with that partner would thus lower our risk?
- Convoy Procedures: Are other NGOs working in this same geographic area and would coordinating road travel along the route affected by banditry be something of interest to others? Would traveling in a group reduce the risk for all.
- Route Security protocols: Is it possible to receive more real-time information about the threat of banditry along our operational routes, and make travel decisions the morning of travel? Are travel itineraries along this route being kept on a strictly need-to-know basis? Is there a pattern to the banditry incidents that are taking place, such that risk can be reduced by avoiding travel at certain times of day? Or, is there really no warning and an assault can take place at any time along the route?
- Hardening the Target (protection strategy): Would the purchase of an armored vehicle be warranted in order to be able to reach certain high priority destinations by adding some additional protection for vehicle passengers?

If CRS has put in place all possible SOPs to try to reduce risk and the risk is still considered to be "high," CRS might want to re-evaluate continued operations in the area(s) where banditry is so prevalent and violent in nature.

B. Contingency Protocols are protocols developed in case a specific security event occurs. As a general principle, contingency protocols should be developed for those threats that occur in the "highly likely-high impact" quadrant (upper right hand corner) of the Risk Rating Matrix. Staff training and practice of contingency protocols for safety and security threats that can cause serious injury or death (such as vehicle accidents; carjacking; abduction; earthquakes; illegal checkpoints; medical emergency or fire) can greatly improve the chances of survivability and therefore reduce risk.

See Chapter 10: Dangerous Situations for additional general guidance and suggested protocols for some of the high impact threats CRS personnel might encounter in the field.

Medical Evacuation

- Give contacts of reputable medical facilities, medical NGOs in the area or U.S. Embassy medical staff who could give a diagnosis.
- SOS offers medical contacts and information on how to start the procedures.

Death Of Staff Or Dependent

- Know how to use the local channels to respect the procedures and traditions in case of the death of a national staff.
- Obtain copies of all necessary documents for insurance claims.
- When an expatriate staff dies:
  - The Regional Director/HQ Human Resources must inform the next-of-kin as soon as

possible and then send a letter of sympathy to the family.
- CRS pays the cost of transporting the deceased back to the employee's point of origin; in this regard the respective consular office affiliated with the deceased person must be contacted as well as the local authorities (for organizational and legal aspects).
- *Consult an airline about procedures and flights.*

If a spouse or child dies, the first concern of all staff should be to support the surviving spouse or parents.

C. Security Levels

Each country program plan should include a stand alone document that outlines the indicators and additional operating procedures for different security phases, as the basic rules for a "normal" situation may not necessarily be the same as for a "crisis" situation. The following five security levels are defined in a standard way in terms of their management/operational implications, i.e. Level III in one country should be equivalent to Level III in another country. In other words, when the Security Level indicates a very restricted operational environment, there are extremely tight movement protocols are in place, pre-evacuation and "hunker down" preparations are ready, and personnel/visitors are restricted to essential business only in order to reduce exposure:

1. Normal.
2. Normal/Restricted.
3. Very Tense.
4. Evacuation.
5. "Under Siege/Hunker Down" (i.e., cannot evacuate safely).

While the implications may be the same from country to country and region to region, the descriptors for each Security Level, triggers for moving from one Security Level to another, and actions to be taken in each Level will vary depending on the country context. The Security Level document serves as a management tool that:

1) Communicates internally (CP, Region, and HQ) the current status of CRS operational environment in any given country at any point in time.
2) Communicates additional standard operating procedures that are added (or taken away) as the country moves between Security Levels.

For Each Security Level:

- List the descriptive indicators—how do we know we are in Security Level I or II?
- List the consequences (e.g., economic activities are reduced).
- List the changes in SOPs and security management measures that will be taken at the different Levels.
- Designate frequency of internal meetings and out-reporting for each level.

A country program may designate different (sub-) office locations as having different Security Levels in effect.

TIP

Depending on the number and accessibility of evacuation options, the number of expatriates and dependents in country, and the acceptable risk threshold in effect in each country, the moment when the evacuation process is implemented may differ by country. If for example, there are a number of third country nationals posted to x country (more difficult to evacuate at the last minute), or a large number of dependents,

or a lower acceptable risk threshold (i.e. the nature of CRS programming is not life-saving), it may make sense to begin withdrawing international staff and dependents earlier rather than later, and the "phased" withdrawal of staff can be described within the Security Levels document.An example of a Security Levels document is included in Chapter 13 Appendices section of these guidelines.

D. Constant Companion

The Constant Companion is a standalone document that every staff person carries with him or her *at all times.* It is a current list of all emergency numbers that any given staff person or visitor might need in case of a safety or security incident. Having these numbers programmed into a cell phone can be helpful, but cell phones are often the first thing to be lost or broken in case of a robbery, vehicle accident, carjacking, etc. In some cases, these emergency numbers can be made into laminated wallet-sized cards to facilitate their portability and durability. The numbers included on each country's Constant Companion will include a mixture of internal CRS and external numbers, depending on the country context these can include: UN Security Officer, U.S. Embassy Regional Security Officer, the SOS medical evacuation call number, local police or fire emergency responder numbers, phone number and address of the nearest hospital/emergency clinic, etc. Information contained in the Constant Companion will be updated annually.See Chapter 13 Appendices section for a sample Constant Companion.

E. Communication Tree

A communications tree is not the same as an organigram. The communications tree illustrates how communications outside of business hours might be rapidly transmitted to all country program staff, with each staff person passing along a message (example: "office closed tomorrow") to approximately 3-5 others, until all staff is reached. It is also a mechanism that can be used in reverse to report back to the CR that all are safe, for example in case of a natural disaster. The use of radios, text messages, in-person home visits, as well as cell phones can be used to transmit communications. The diagram of the communications tree illustrates who is responsible for contacting whom down the tree and reporting back up the tree to whom.

See Chapter 13 Appendices section for a sample Communications Tree.

F. Relevant Maps

The following are considered critical to a country program's Field Security Plan include:

- City map highlighting "safe haven" locations.
- Office layout map illustrating location of fire exits, exit routes for different office clusters, and exterior rendezvous points.
- Map illustrating "coded" locations if radio communications protocols demand regular check-ins for staff movement where perpetrators may be listening in and interested to know CRS locations and destinations. (In this case, maps would be kept very confidential, and codes changed from time to time).
- Map illustrating rendezvous locations and protocols in case a "No Communications" protocol is warranted (see Chapter7 for additional guidance on No Communications protocols).
- See Chapter 13 Appendices Section for Using Map and Compass Together.

G. Rapid Risk Assessment Matrix (Recommended for Volatile Environments)

Some country programs are operating in a security environment that is changing rapidly and constantly, requiring ongoing monitoring of how new trends affect risk to CRS and therefore affect standard operating procedures in place from one day to the next. This tool facilitates the constant and systematic monitoring and communication of changes to the country

program's risk assessment for volatile environments, adapted from the UN Security Risk Assessment (SRA).

Threat	Vulnerability		Risk Rating	New Actions	Risk
List each Threat on separate line.	Strength (Factors and SOPs that reduce CRS vulnerability)	Weakness (Factors and SOPs that increase CRS vulnerability)	(Current)	To further mitigate risk	(Post-Action)

This format represents a summarized version of what otherwise would go into the text of the Threat, Vulnerability and Risk Assessment section of the Field Security Plan. This shortened version enables country program management to focus on the connection between policies and procedures in place and the threats and vulnerabilities they are designed to address. As the threat changes (i.e. the frequency of attacks increases, or the location of attacks gets closer to CRS operational sites), this tool should prompt country program management to think through how our vulnerability and risk changes, and to identify new SOPs that will effectively reduce risk given those changes. The New Actions column gives country management a way to document and communicate to staff those procedures which are changing and why, and also to follow up on actions delegated to others for implementation.

The use of this matrix as a management tool decreases the necessity that the full Threat, Vulnerability and Risk Assessment process and document remain current, while that "heavier" document can continue to be updated annually in a more complete way.

H. Evacuation Plans

Every CRS field program operating in any environment must foresee the possibility of an evacuation. The evacuation plan is a detailed stand-alone document, and is not shared with everyone on staff, but only with those who are to be evacuated or who have a role in preparing for and implementing an evacuation. There are evacuation options that will involve following the UN or foreign embassy's plan. CRS will not always be able to foresee exactly how the evacuation will take place. However to the extent that CRS staff are prepared for an evacuation of any sort and the national staff are clear about who is responsible for what in the absence of international staff, the better. The objective of an evacuation plan is two-fold:

1. It facilitates an orderly and rapid departure in an insecure environment in order to limit security risks.
2. It informs each individual about the "when, how and who" of an evacuation.

Format Of An Evacuation Plan (maximum 5 pages)
Country Program:
Region:
Plan Updated:
Country Representative:
Security Focal Point:
Number of International Staff:
Number of Dependents:
Number of National Staff:

CRS Staff included in this Evacuation Plan:

Employee/Family	Position	Essential/Non-Essential Status	Priority Level Status (see definitions below)

In addition to the staff noted above, this plan is provided to the following persons:

Name	Position	Location

Approvals:
Country Representative: XX/Date
RTA/Security: XX/Date
Regional Director: XX/Date

Definition of Evacuation Priority Levels (ECHO categories)
- **Priority 1** - International Staff family members.
- **Priority 2** - Staff members who are in immediate personal danger due to the conditions of the crisis.
- **Priority 3** - Individuals other than essential staff (i.e. third country nationals, nationals without diplomatic representation).
- **Priority 4** - Essential staff.

Introduction
- Summary of Evacuation Policy, Decision-making authority and Consequences of non-compliance.
- Criteria/Triggers for Evacuation.
- Personal Grab-bag Items and Luggage Requirements.
- Other Evacuation Preparation Task Assignments.
- Evacuation/Relocation Scenarios.
- Temporary/Permanent Relocation of Offices (under what circumstances, to what location, "business continuity" provisions, etc.).
- Evacuation/Relocation of Staff and/or Dependents (phases, collection points, to what location, communication means, etc.).
- List of Evacuation Options/Routes (in order of preference, describe what assumptions, preconditions will need to be in place for each option to be successful).
- Level V: Under Siege/Hunker Down (describe special instructions, collection point, etc.).

Post-Evacuation Plan
- Describe provisions for business continuity after internationals have evacuated.
- Designate national staff roles and responsibilities in this scenario.
- Decision to Return: describe how this decision will be made.

Key points related to the evacuation plan:
- The plan should be unambiguous and understood by all CRS members.
- The evacuation section of the country program field security plan should be kept in a secure place.
- The plan should be discussed during meetings within the team and kept up-to-date.
- Copies should be sent to the regional RD and RTA/Emergency-Security, as well as the OSD-RR and Director of Staff Safety and Security at HQ.

In the case of an evacuation that does not include national staff, they should be:
- Informed of the situation.
- Paid and given salary advances if appropriate.
- Tasked with responsibilities if appropriate (e.g., decision-making authority regarding programming and management of the office).
- Supported as possible with emergency supplies such as food and water.
- Protected from attack by removing any personal data on national staff to a safe location.

1. Boarding List : List of evacuees, including name, gender, nationality, age, blood type.
- List of kilos carried per person.
- Total kilos of the evacuation kit for the team.
- CRS mission statement with local translation.
- Channel and call signs for radio communications.
- Emergency contact list.
- Maps identifying each evacuee's residence, group meeting points, and evacuation roads by color code (e.g. blue = road to north, green = road to south, etc.).

  For evacuation by road:
  - List of evacuees, including name, gender, nationality, age, blood type.
  - Identify an international staff driver per vehicle.
  - Include, if possible, a medical person per vehicle.
  - Include at least 2 persons per vehicle.
  - Specify the place order of each vehicle in the convoy.

2. Assignment Of Tasks

Each international staff is responsible for bringing minimal personal baggage and ensuring that important documents are included. Good preparation will avoid excessive work at the time of evacuation.

Tasks include:
- coordination of the evacuation.
- communication with national staff.
- communication with local authorities.
- management of computer hardware, software and data files/disks (i.e., erase data on hard disk for abandoned material, if deemed appropriate).
- management of money and accountancy.
- management of radio equipment (erase frequencies on abandoned material).
- collection of work contracts and leases to take.

- collection of equipment inventories to take.
- preparation of supplies for evacuation such as medical, survival, and evacuation kits.
- preparation of vehicles for a road evacuation or distributing vehicles to national staff, local counterparts, etc. if evacuating by other means.
- removal of CRS identification from buildings and abandoned vehicles.

3. Evacuation Kit Per Vehicle

Standard kits should be prepared for each vehicle in the case of an evacuation by road. *The kits should be prepared in advance and maintained.* Kits will need to be designed according to the specific needs of the operating environment. Included below is a list of items that could be included in a vehicle evacuation kit.

Evacuation Kit Contents (suggested)

- ✓ a plan or a map of the itinerary and a compass
- ✓ CRS flag
- ✓ Torch-lamp with spare batteries/bulbs
- ✓ 1 jerrycan of water (20 liters)
- ✓ 2 cans of 5 liters motor oil and a filter
- ✓ 1 liter of brake fluid
- ✓ 1 roll of metal wire
- ✓ 1 winch
- ✓ 2 machetes
- ✓ Potable water (10 liters)
- ✓ 5 matchboxes
- ✓ 6 survival blankets
- ✓ 50 chloramine tablets
- ✓ first aid kit
- ✓ identification
- ✓ 2 jerrycans of gas and a funnel
- ✓ 1 fan belt
- ✓ 1 gas filter
- ✓ 1 set of fuses (for vehicle)
- ✓ 1 set of snow chains, if appropriate
- ✓ 1 big rope, 20 meters long
- ✓ 1 shovel
- ✓ dry biscuits
- ✓ 4 rolls of toilet paper
- ✓ 1 plastic sheeting (4x5m)

In case of evacuation by other means of transport (boat, aircraft, by foot), individual "grab bags" should be developed according to the maximum load allowed.

Sample Checklist for 'Grab Bag' Contents

Technical Equipment

- ✓ Sat-phone
- ✓ GPS & Compass
- ✓ VHF handset, batteries and charger
- ✓ Laptop computer - if space permits
- ✓ SW radio receiver
- ✓ Torch/flashlight

Documents
- ✓ Passport
- ✓ Vaccination and other health certificates
- ✓ Return tickets (if relevant)
- ✓ Money - Dollars and currency of host and asylum country
- ✓ Insurance documents
- ✓ Medical evacuation card (SOS)
- ✓ Drivers license
- ✓ Contact list and personal address book
- ✓ Ball point pen and note book

Clothing
- ✓ At least one complete change of clothing
- ✓ Underwear and socks
- ✓ Towel
- ✓ Sun hat/sun glasses

Medicines & Toiletries
- ✓ Anti-malarial drugs and treatment
- ✓ Mosquito repellent
- ✓ Sun block
- ✓ Toilet paper
- ✓ First aid kit w/ sterile needles
- ✓ Water purification tablets
- ✓ Wash kit
- ✓ Emergency anti-diarrheal drugs
- ✓ Oral re-hydration salts
- ✓ Glasses/contact lenses
- ✓ Contact lens cleaning fluid
- ✓ Comb/hairbrush
- ✓ Tampons
- ✓ Personal prescription medicines

Food and Drink
- ✓ At least 1 litre of water
- ✓ Survival rations
- ✓ Chocolate or high energy bars
- ✓ High energy drinks

Communicate And Practice

Having a written security plan is not enough! Following a review and approval of the plan at the regional level, time should be allotted for communicating the contents of the plan to all staff. All staff should read the Field Security Plan and sign the "Staff Statement of Understanding of Security Guidelines" form found in Chapter 11: Forms and Graphics. If staff is illiterate, all sections of Field Security Plan should be reviewed orally with them. The objective of the communication should be that all staff is aware of what CRS security management policies and procedures are, and what their rights and responsibilities are with respect to the implementation of these policies and procedures.

Finally, from time to time, the CR and Security Point Person should organize drills on various aspects of the plan—from fire drills and practice using fire extinguishers, to evacuation preparedness drills. Drills can be a creative and fun way to reinforce and refresh CRS security protocols, and can help to make "second nature" behaviors that might otherwise not come naturally in the heat of a safety or security event.