PROTECTION HANDBOOK FOR HUMAN RIGHTS DEFENDERS

Human rights defenders are the people whose legitimate work for human rights creates the building blocks of societies based on the principles of justice, equality and human rights.

This handbook is intended to give human rights defenders at risk practical advice on how to deal with the attacks which they may have to deal with in their work as a human rights defender.

This manual is designed as a quick reference handbook giving helpful and practical suggestions on steps to improve personal security.

Front Line seeks to provide 24 hour support to human rights defenders at immediate risk. If you are a human rights defender and are concerned about your personal safety please feel free to contact our emergency number at any time. After office hours you will be offered five language options, each of which will connect you to a member of staff.

Our emergency number can be contacted at any hour on

+353 1 21 00 489

WWW.FRONTLINEDEFENDERS.ORG

This handbook was produced with the generous support of Irish Aid

Irish Aid
Department of Foreign Affairs
An Roinn Gnóthaí Eachtracha

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

81 Main St, Blackrock,
Co. Dublin, Ireland
Tel 00 353 1 212 37 50
Fax 00 353 1 212 10 01

ISBN 978-0-9554389-1-2

9 780955 438912 >

PROTECTION HANDBOOK FOR HUMAN RIGHTS DEFENDERS

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

PROTECTION HANDBOOK FOR HUMAN RIGHTS DEFENDERS

PUBLISHED BY

FRONT LINE
THE INTERNATIONAL FOUNDATION
FOR THE PROTECTION OF
HUMAN RIGHTS DEFENDERS

EDITED BY

ARNOLD TSUNGA,
EXECUTIVE DIRECTOR,
ZIMBABWE LAWYERS FOR HUMAN RIGHTS

Front Line
PROTECTION OF HUMAN RIGHTS DEFENDERS

Published in November 2007 by Front Line
The International Foundation
for the Protection of Human Rights Defenders

81 Main St, Blackrock, County Dublin, Ireland

Copies of this handbook are available from:
info@frontlinedefenders.org
Price €10 plus post and packaging

This publications is also available online at:
www.frontlinedefenders.org/manuals/protection-booklet

To request/order a copy please contact:

Front Line
The International Foundation for the
Protection of Human Rights Defenders
81 Main St, Blackrock, County Dublin, Ireland
Tel 00 353 1 212 37 50
Fax 00 353 1 212 10 01

This manual is being translated into French, Spanish, Russian and Arabic by Front Line.

ISBN: 978-0-9554389-1-2

FRONT LINE

Front Line was founded in Dublin in 2001 with the specific aim of protecting Human Rights Defenders, people who work, non-violently, for any or all of the rights enshrined in the Universal Declaration of Human Rights (UDHR).

Front Line aims to address some of the needs identified by defenders themselves, including protection, networking, training and access to international bodies that can take action on their behalf.

Front Line seeks to provide rapid and practical support to at-risk human rights defenders, including through a 24 hour emergency response phone line, and through promoting the visibility and recognition of human rights defenders as a vulnerable group.

Front Line runs a small grants program to provide for the security needs of defenders. Front Line mobilises campaigning and lobbying on behalf of defenders at immediate risk. In emergency situations Front Line can facilitate temporary relocation.

Front Line conducts research and publishes reports on the situation of human rights defenders in specific countries. The organisation also develops resource materials and training packages on behalf of human rights defenders as well as facilitating networking and exchange between defenders in different parts of the world.

Front Line promotes strengthened international and regional measures to protect human rights defenders including through support for the work of the UN Special Representative on Human Rights Defenders. Front Line seeks to promote respect for the UN Declaration on Human Rights Defenders.

If there are aspects of personal security which you feel are

not adequately addressed in this, or other Front Line publications, we would be very happy to hear from you. Please feel free to contact us at **info@frontlinedefenders.org**

For general information on the work of Front Line please log onto **WWW.FRONTLINEDEFENDERS.ORG**

Front Line has Special Consultative Status with the Economic and Social Council of the United Nations.

Front Line is the winner of the 2007 King Baudouin International Development Prize.

ACKNOWLEDGEMENTS

The Front Line Protection Handbook is largely based on the excellent work of Enrique Eguren of Peace Brigades International in the *Protection Manual for Human Rights Defenders*[1] (Front Line, 2005).

This handbook is an attempt to summarise and adapt the 'Protection Manual' in a more compact form which can be more readily distributed and used by human rights defenders.

Front Line is grateful for the ongoing and generous support of Irish Aid and the Irish Department of Foreign Affairs.

Editor
Arnold Tsunga is the Executive Director of Zimbabwe Lawyers for Human Rights (ZLHR) and the winner of the 2006 Martin Ennals Prize.[2] In addition to his personal experience as a human rights defender at risk Arnold has been responsible for organising security training for human rights defenders in Zimbabwe.

Human Rights Defenders
Front Line defines a human rights defender as "a person who works, non-violently, for any or all of the rights enshrined in the Universal Declaration of Human Rights." Front Line seeks to promote the UN Declaration on Human Rights Defenders (1998).[3]

Footnotes are found at the end of the handbook.

INTRODUCTION

Dear Friends
This handbook is intended to give you practical advice on how to deal with the threats, intimidation and attacks, which you may have to deal with in your work as a human rights defender.

When I talk to human rights defenders I often find that they are so focused on the work of their community or organisation that their own safety is of secondary importance. Some even seem to accept that danger is simply part of the job. However, there are many simple and practical steps that you can take to reduce the risk and which we hope will help to keep you safe.

Front Line believes that human rights defenders are key agents of change and that the only way to ensure long term sustainable development based on human rights, is to create a safe space in which human rights defenders, like you, can work safely, without the threat of arrest or intimidation.

Front Line is dedicated to the protection of human rights defenders at risk. Our specific aim is to provide round the clock practical support, so that defenders can continue their work safely. We try to help human rights defenders manage and cope with the risks that they face.

As part of our work with human rights defenders we deliver regional and international training in personal security, risk assessment and IT security. Front Line also works with women human rights defenders to address the specific risks they face.

In addition to providing security training on the ground, Front Line has also developed a series of personal and digital security manuals which are intended as practical tools to help defenders deal with and overcome the threats that they face. You can find all of these resources on our web site at:

WWW.FRONTLINEDEFENDERS.ORG

This handbook is designed as a quick reference tool in which you will find helpful and practical suggestions on steps to improve your personal security situation. The most important thing is that you are able to continue your work for the protection of the human rights of others.

In the words of anthropologist Margaret Mead “Never doubt that a small group of thoughtful, committed citizens can change the world. Indeed, it is the only thing that ever has”.

Yours sincerely
Mary Lawlor,
Director, Front Line

CONTENTS

CHAPTER 1:
WHY WORRY ABOUT THE PROTECTION OF HRDS? 1

CHAPTER 2:
ASSESSING RISK: THREATS, VULNERABILITIES AND CAPACITIES 3

CHAPTER 3:
UNDERSTANDING AND ASSESSING THREATS 9

CHAPTER 4:
SECURITY INCIDENTS 11

CHAPTER 5:
PREVENTING AND REACTING TO ATTACKS 15

CONCLUSION 18

SECURITY CHECKLIST 22

1 WHY WORRY ABOUT THE PROTECTION OF HRDS?

"Human rights defenders carry out the vital work of protecting everyone's rights. Protection of such defenders thus takes on singular importance."[4]
Inter-American Commission on Human Rights

Many Human Rights Defenders (HRDs) are uncomfortable with a focus on their own protection because their purpose is to defend the rights of others. However, precisely because HRDs are on the frontline defending other people's rights, HRDs often find themselves being targets of persecution. If there is no security for HRDs to undertake their legitimate work then there will be no effective protection for the rights of anyone.

Front Line is concerned about the security and safety of HRDs because attacks committed against HRDs are not indiscriminate. In most cases, threats and violence are a deliberate and well-planned response to defenders' work, and linked to a clear political or military agenda.

The UN Declaration on Human Rights Defenders stresses that the state has a primary responsibility for protecting human rights defenders.

WHY THIS HRDS' HANDBOOK?

This handbook is specifically targeted at human rights defenders (HRDs). It is aimed at:

- Giving HRDs a quick reference handbook with additional knowledge and some tools to deal with their everyday security and protection concerns
- Helping HRDs to undertake their own risk assessments to gain a fuller appreciation of the threats they face, their vulnerabilities, and the capacities they have to deal with

those threats and reduce the risk or exposure to the risk

- Helping HRDs define their own security rules and procedures which suit their particular situation so as to mainstream security and protection in their day to day work
- Facilitating the development of a set of strategies aimed at improving HRDs' security management
- Encouraging HRDs to adopt a structured response towards their own safety and security and to go beyond people's individual knowledge about security and moving towards an organisational culture in which security is inherent
- Allowing NGOs and HRDs to plan for and cope with the increasing security challenges involved in human rights work
- Contributing ultimately towards the preservation of the invaluable work that human rights defenders do

It aims to provide a very basic tool box for HRDs to improve their security and protection.[5]

2 ASSESSING RISK: THREATS, VULNERABILITIES AND CAPACITIES

PURPOSE:

This section seeks to explain the following key concepts: risk, threats, vulnerability and capacity in terms of security. It is impossible to have an effective security and protection strategy in the absence of an adequate understanding of these concepts.

Key Concepts:

Risk refers to the possibility of events, however uncertain, that will result in harm.

In order to develop and implement protection strategies HRDs must analyse what levels of risk they face.

Threats are indications that someone will harm somebody else's physical or moral integrity or property through purposeful and often violent action.

Vulnerability refers to the factors that can make it more likely that a HRD or a group will suffer an attack or will suffer greater harm as a result of an attack.

Capacities are the strengths and resources a group or a HRD can access to improve their security and/or survive an attack.

RISK ELABORATED

The level of risk facing a group of defenders increases in accordance with threats that have been received and their vulnerability to those threats, as presented in this equation:[6]

RISK = threats x vulnerabilities

The risk created by threats and vulnerabilities can be reduced if defenders have enough capacities (the more capacities, the lesser the risk).

$$\text{RISK} = \frac{\text{threats x vulnerability}}{\text{capacities}}$$

In summary, in order to reduce risk to acceptable levels – namely, to protect – you must:

- Reduce threats (where possible);
- Reduce vulnerability factors;
- Increase protection capacities.

Generally speaking HRDs can have more immediate impact on their own capacities and vulnerabilities whilst reducing threats might need to be a more long-term strategy.

NB: Risk must be assessed periodically as working environment, threats or vulnerabilities change.

Threats Elaborated

There are different types of threats;

- **Indirect threats** often resulting from criminal activity or armed conflict
- **Targeted threats** usually closely related to the work of the HRDs in question, as well as to the interests and sensitivities of the people who are opposed to the HRDs' work

Targeted threats are the most common and seek to hinder or change a group's work, or to influence the behaviour of the people involved.

VULNERABILITY AND CAPACITY ELABORATED

Vulnerability depends on circumstances. Some factors that increase or reduce vulnerability include access or lack of access to:

- Effective and secure means of communication
- Safe ground transportation
- Proper locks or other security for a house or office
- Support from other HRDs through networks or a system for joint responses when HRDs are attacked

Capacities and vulnerabilities are two sides of the same coin. For example, not knowing enough about your work environment is a vulnerability, while having this knowledge is a capacity.

NB: Vulnerabilities and capacities, as well as some threats, may vary according to gender, age or other factors.

REDUCTION OF THREATS

Threats or exposure to threats can be reduced by:

- Increasing the political cost of carrying out such threats, for example, through publicising the threat extensively by generating a response by domestic and international networks of HRDs to the threats
- Increasing the perception that an attacker might be caught and punished
- Increasing the perception that the political cost of acting openly against a HRD far outweighs the benefit
- Persuading powerful interests that respect for international human rights standards is desirable and that the State has a duty to protect
- Increasing lobbying and advocacy for the strengthening of the rule of law necessary to fight impunity
- Developing, in appropriate cases, contacts with the authorities, police, army etc.

NB: This last point has its own pros and cons. Advantages could be early warning or dissuasion – disadvantages could be allegations of compromising security, leaking, being untrustworthy – also authorities/security services playing games, divide and rule, etc.

COPING STRATEGIES

Different people cope in different ways, ranging from a fully thought out response to outright denial or the counter-productive.

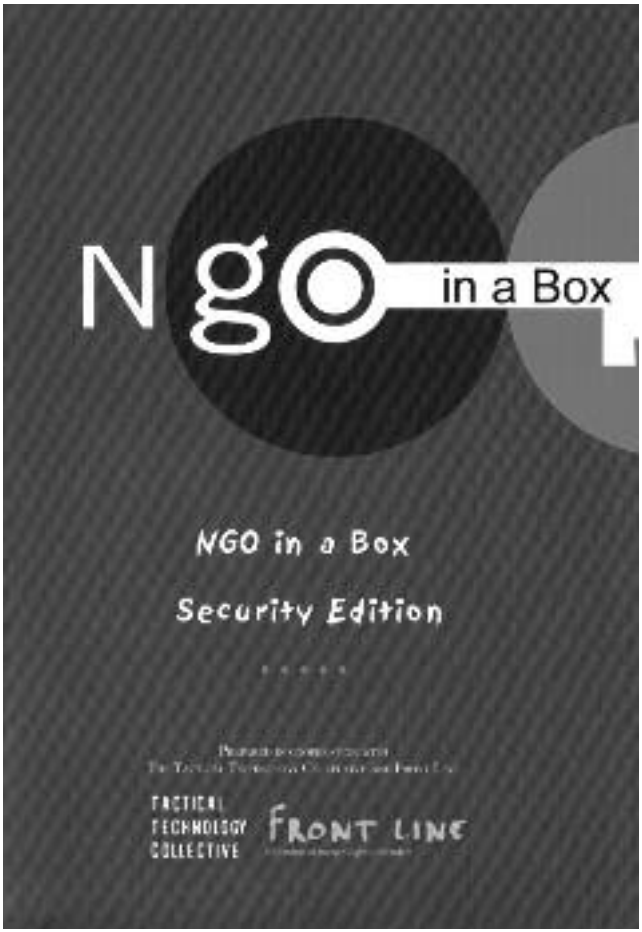
Some coping strategies:

- Reinforcing protective barriers, hiding valuables
- Avoiding behaviour which could be questioned
- Going into hiding during high risk situations
- Looking for appropriate protection from one of the actors
- Suspending activities, closing down the office, evacuating. Forced migration (internal displacement or as refugees) or going into exile
- Relying on “good luck” or resorting to “magic” beliefs
- Becoming more secretive, including with colleagues; going into denial by refusing to discuss threats; excessive drinking, overwork, erratic behaviour

NB: Bear in mind that in some cases the response strategies might even create more security problems than those they were intended to address. So reflect critically and consider ramifications before you settle for a specific coping strategy.

COPING AND RESPONSE STRATEGIES MUST TAKE THE FOLLOWING INTO ACCOUNT:

- Sensitivity: Can your strategies respond quickly to individual or group security needs?
- Adaptability: Can your strategies be quickly adapted to new circumstances, once the risk of attack is over?
- Sustainability: Can your strategies endure over time, despite threats or non-lethal attacks?
- Effectiveness: Can your strategies adequately protect the people or groups in question?
- Reversibility: If your strategies don’t work or the situation changes, can your strategies be reversed or changed?



3. UNDERSTANDING AND ASSESSING THREATS

PURPOSE:

This section aims to provide an understanding of threats and how to respond to them. The two main objectives when assessing a threat are:

- To get as much information as possible about the purpose and source of the threat (both will be linked to the impact of your work)
- To reach a reasonable conclusion about whether the threat will be acted on or not

ADDITIONAL CONCEPTS ON THREATS

Declared Threat is a declaration or indication of an intention to inflict damage, punish or hurt, usually in order to achieve something.

Possible Threat arises when threats or attacks against others suggest you might be threatened or attacked next.

DEALING WITH DECLARED THREATS

IDENTIFYING SOURCE OF THREAT

The **source of threat** is almost always the person or group who has been affected by the defender's work. A threat also has an **objective** which is linked to the impact of the defender's work. Receiving a threat therefore represents feedback on how your work is affecting someone else.

UNDERSTAND "MAKING" VS "POSING" A THREAT

Anyone can make a threat, but not everyone can pose a threat. Some people who **make** threats ultimately **pose** a threat. Many people who **make** threats **do not pose** a threat. Some people who **never make** threats **do pose** a threat.

You need to assess the capacity of the person making a threat to act against you. You need to know if the threat can be put into action so that you take action to protect yourself.

It is useful to think about why someone has made a threat rather than taken direct action against you. It is often 'cheaper' in terms of time, effort and resources to make a threat. There is perhaps less chance of being identified as a perpetrator. Whenever a threat is made it is evidence that a calculation of potential cost and benefit has been made. This does not mean that the perpetrator may not eventually take direct action but analysing why a threat has been made in a specific way at a specific time can give very valuable information for a protection strategy.

Five steps to assessing a threat

1. Establish the facts surrounding the threat(s).
2. Establish whether there is a pattern of threats over time.
3. Establish the objective of the threat.
4. Establish who is making the threat.
5. Make a reasonable conclusion about whether or not the threat can be put into action.

There are good reasons for following the order of the steps. Going directly to step 2 or 4, for example, will miss out the more solid information arising from the previous steps.

Maintaining and closing a threat case

You can consider closing a threat case when the potential attacker is deemed to no longer pose a threat.

It is in the nature of threats to increase the stress levels of those who are threatened. Try to be conscious of and find ways to manage the impact of stress on yourself and colleagues.

4. SECURITY INCIDENTS 4

PURPOSE:

This section seeks to explain how to recognise and respond to security incidents.

A DEFINITION OF SECURITY INCIDENT

A **security incident** is any fact or event which you think could affect your personal or organisational security. All threats are security incidents, but not all security incidents are threats. Security incidents represent "the minimum unit" of security measurement and indicate the resistance/pressure on your work. **Do not let them go unnoticed!**

Some examples of security incidents:

- seeing the same, suspicious vehicle parked outside your office or home over a number of days
- the telephone ringing at night with nobody at the other end
- somebody asking questions about you in a nearby town or village
- someone stalking you
- a break-in at your house
- someone threatening you in a bus queue, etc.

Why are security incidents so important?

Security incidents **provide**:

- vital information about the impact your work is having
- vital information about possible action which may be planned or carried out against you
- opportunities to avoid places which could be dangerous, or more dangerous than normal
- Opportunities to change your behaviour or activities. For instance, you may realise that you are under surveillance after noticing several security incidents: now you can take action about surveillance.

Analysis of Security Incidents

You notice something **>** you realise it might be a security incident **>** you register / share it **>** you analyse it **>** you establish that it is a security incident **>** you react appropriately.

In urgent cases this sequence should still take place, just much more quickly than usual to avoid delay.

NB: If several seemingly minor incidents affecting different people are not routinely noted and shared then the organisation will be less well prepared and more vulnerable to an escalation of harassment or attacks.

DEALING WITH SECURITY INCIDENTS

- Developing and maintaining an up-to-date checklist, such as that on page 16, to deal with security issues in a systematic manner should cover the following:
  1. The organisation's information management systems dealing with communications (not only electronic but other materials also) in a secure manner.[7]
  2. Maintaining a list of HRDs and international networks (including UN and regional agencies) that need to be provided with advocacy alerts when attacks seem possible or imminent.
  3. Who to contact in an emergency in respect of every HRD?
  4. Who should have the emergency contacts (someone who won't be arrested/attacked)?
  5. Recovery plan (should be tested in practice)

Do not forget that it is more common that security incidents are overlooked or dismissed. Deal with security incidents in three basic steps:

1. Register them in a security incidents book
2. Analyse them
3. React to them as appropriate

Prompt action is important, but knowing **why** you are taking action is more important.

The following steps have been suggested.

- Step 1: Report the incident in detail and factually.
- Step 2: Make a decision whether and when to react: your **immediate reaction** may be followed by **rapid reaction** (in the next few hours or days) and then a **follow up action** (in several days, weeks or even months)
- Step 3. Decide how to react and what your objectives are.

NB: Any reaction has to take into account the security and protection of other people or organisations or institutions with which you have a working relationship.

5. PREVENTING AND REACTING TO ATTACKS

PURPOSE:

This section seeks to explain how to:

- Assess the likelihood of different kinds of attacks taking place
- Prevent possible direct attacks against HRDs
- Carry out counter-surveillance measures to improve security (if appropriate)

ATTACKS AGAINST HRDS

Attacking is a process, as well as an act. Careful analysis of attacks often shows that they are the culmination of conflicts, disputes, threats and mistakes which have developed and can be traced over time.

Attacks against HRDs are the product of at least three interacting factors:

1. *The individual attacker*. Attacks on HRDs are often the product of processes of thought and behaviour we can understand and learn from even if they are illegitimate.
2. *Background and triggers which lead the attacker to see the attack as an option*. Most people who attack HRDs see attacking as a way of reaching a goal or solving a problem.
3. *A setting* that facilitates the attack.

WHO, THEN, IS A DANGER TO HRDS?

Generally, anyone who thinks that attacking a HRD is a desirable or a potentially effective way to achieve a goal.

Surveillance and Counter-Surveillance

Attackers usually plan an attack after gathering information about their target in terms of the right method, place, time

and resources to attack and escape. Surveillance of HRDs usually takes place at their workplace, homes or places where they socialise. Attacks are carried out at HRDs' moments of greatest vulnerability and weakest capacity. Anyone in your area, such as doormen or porters in buildings, travelling sales people who work close to the building entrance, people in nearby vehicles, visitors, etc., could potentially all be watching your movements.

Try **counter surveillance** by:

- Subtly watching those who could be watching you
- Noticing movements of people in your area and changes in their attitude
- Involving a trusted third party to watch them for you without confronting them or letting them know
- Before arriving home you can ask a family member or trusted neighbour to take up a position close by (e.g. changing a car wheel), to check if somebody is awaiting your arrival
- Identifying and analysing security incidents

You must know that:

- Attacking a HRD isn't easy and requires resources and planning
- People who attack HRDs usually show a degree of consistency
- Geographical factors matter
- Choices and decisions are made before an attack

PREVENTING A POSSIBLE DIRECT ATTACK

If the risk of attack is high:

- Immediately and effectively confront the threat if you can prevent the attack
- Reduce your exposure to as close to zero as possible, by going into hiding or leaving the area
- Seek appropriate protection from appropriate bodies e.g. diplomatic protection from friendly embassy staff in your country to exit the country or a part of the country where you are targeted
- One option is sometimes to get protection from the authorities or international bodies (e.g. UN peacekeepers)
- Try to avoid as much as possible having a predictable routine
- Try to maintain a high level of alertness. Try to be conscious of and find ways to manage the impact of stress on yourself and colleagues
- Inform other HRDs who may be able to help and who may also be at risk

Reacting to attacks

In any kind of attack:

- Go for the safest option available
- Take action to solve the situation, and restore a safe work environment for you and your organisation
- Immediately record as much detailed information as possible about the attack: What happened, who/how many people were involved, number plates of vehicles, descriptions, etc.
- Keep copies of any documents handed over to the authorities to document the case
- Immediately contact your lawyer to take remedial action if appropriate and possible, even if there is no immediate prospect of redress. It can be helpful in pursuing regional or international action to have demonstrated an attempt to make a national level complaint
- Seek medical attention from your doctor or a reputable and trusted network offering psychosocial support and record medical condition

CONCLUSION

This handbook dealt with and explained the key concepts in the field of the security of HRDs such as threats, vulnerability and capacity. It also showed the relationship between vulnerabilities and capacities and their interplay with threats. Vulnerabilities and capacities fall within the internal sphere of HRDs and can be addressed by the HRD quite quickly. Threats emanate from the external environment and need longer term strategies to address them effectively.

Reducing vulnerabilities and increasing capacities does not reduce the threats. If the political consequences of carrying out a threat outweigh the benefit of effecting the threat, then it is unlikely to be carried out and the threat factor is reduced. To effectively track the threat factor it was emphasised that security incidents must never go unnoticed as they provide useful feedback on your work and highlight possible areas of vulnerabilities.

Planning for improved security is fundamental to recognising the importance of the work of HRDs and the need to ensure continuity of the work. Above all it is a recognition of our responsibility not just to protect ourselves but also to protect our friends, family, colleagues and the people on whose behalf we work, who may be at risk.

This publication cannot be considered a definitive document and Front Line would welcome feedback on strategies or approaches that you have used and found effective. We can then share this information with our colleagues.

Discussing risks does not need to be disempowering. With a structured approach HRDs can find ways to manage risk more effectively, even when it cannot be entirely eliminated.

We end with our risk assessment tool for emphasis.

$$\text{RISK} = \frac{\text{threats x vulnerability}}{\text{capacities}}$$

Footnotes

1. Enrique Eguren, Peace Brigades International, European Office (PBI BEO): *Protection Manual for Human Rights Defenders* (Front Line, 2005) www.frontlinedefenders.org/manuals/protection

2. www.martinennalsaward.org

3. Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognised Human Rights and Fundamental Freedoms

4. Inter-American Commission on Human Rights Press Release 6/02 Washington, D.C., February 15, 2002 on the assassination of Mrs. María del Carmen Florez, human rights defender, which occurred on Thursday, February 14, 2002, in Colombia.

5. The more comprehensive Protection Manual, the more specific Digital Security Manual and *NGO-in-a-Box* can be requested from Front Line by e-mail or phone, or see: www.frontlinedefenders/digital-security

6. Van Brabant (2000) and REDR.

7. Security Edition of the *NGO-in-a-Box* toolkit is available on request.
   See also: www.frontlinedefenders/digital-security

SECURITY CHECKLIST

COMPONENTS OF VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS VULNERABILITIES OR CAPACITIES
GEOGRAPHICAL, PHYSICAL AND TECHNICAL COMPONENTS	
EXPOSURE	The need to be in, or to pass through, dangerous areas to carry out normal daily or occasional activities. Threatening actors in those areas.
PHYSICAL STRUCTURES	The characteristics of housing (offices, homes, shelters); building materials, doors, windows, cupboards. Protective barriers. Night lights.
OFFICES AND PLACES OPEN TO PUBLIC	Are your offices open to visitors from the general public? Are there areas reserved only for personnel? Do you have to deal with unknown people that come to your place?
HIDING PLACES, ESCAPE ROUTES	Are there any hiding places? How accessible are they (physical distance) and to whom (for specific individuals or the whole group)? Can you leave the area for a while if necessary?
ACCESS TO THE AREA	How difficult is it for outside visitors (government officials, NGOs, etc.) to access the area, for example in a dangerous neighbourhood? How difficult is access for threatening actors?
TRANSPORT AND ACCOMMODATION	Do you have access to safe transportation (public or private)? Do these have particular advantages or disadvantages? Do defenders have access to safe accommodation when travelling?
COMMUNICATION	Are telecommunications systems in place (radio, telephone)? Do defenders have easy access to them? Do they work properly at all times? Can they be cut by threatening actors before an attack?
COMPONENTS LINKED TO CONFLICT	
LINKS TO CONFLICT PARTIES	Do you have links with conflict parties (relatives, from the same area, same interests) that could be unfairly used against the defenders?
DEFENDERS' ACTIVITIES AFFECTING A CONFLICT PARTY	Does your work directly affect an actor's interests? (For example, when protecting valuable natural resources, the right to land, or similar potential targets for powerful actors).
VALUABLE GOODS AND WRITTEN INFORMATION	Do you have items or goods that could be valuable to armed groups, and therefore increase the risk of targeting (petrol, humanitarian aid, batteries, human rights manuals, health manuals, etc.)?
KNOWLEDGE ABOUT FIGHTING AND MINED AREAS	Do you have information about the fighting areas that could put you at a risk? And about safe areas to help your security? Do you have reliable information about mined areas?

COMPONENTS OF VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS VULNERABILITIES OR CAPACITIES
COMPONENTS LINKED TO THE LEGAL AND POLITICAL SYSTEM	
ACCESS TO AUTHORITIES AND TO A LEGAL SYSTEM TO CLAIM YOUR RIGHTS	Can you start legal processes to claim their rights? (Access to legal representation, physical presence at trials or meetings, etc.) Can you gain appropriate assistance from relevant authorities for your work and protection needs?
IS YOUR ORGANISATION ABLE TO GET RESULTS FROM THE LEGAL SYSTEM AND FROM AUTHORITIES	Are you legally entitled to claim your rights? Or are you subject to repressive internal laws? Can you gain enough clout to make authorities take note of your claims?
REGISTRATION, CAPACITY TO KEEP ACCOUNTS AND LEGAL STANDARDS	Are you denied legal registration or subjected to long delays? Is your organisation able to keep proper accounts and meet national legal standards? Do you use pirated computer software?
MANAGEMENT OF INFORMATION	
SOURCES AND ACCURACY OF INFORMATION	Do you have reliable sources of information to base accusations on? Do you publicise information with the necessary accuracy and method? Is your data backed up and stored in more than one place separately?
KEEPING, SENDING AND RECEIVING INFORMATION	Can you keep information in a safe and reliable place? Could it get stolen? Can it be protected from viruses and hackers? Can you send and receive information safely?

COMPONENTS OF VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS VULNERABILITIES OR CAPACITIES
MANAGING DIGITAL COMMUNICATION AND INFORMATION STORAGE	Do you keep your computer healthy and secure (anti-virus and malware software, firewall, updating all software)? Do you ensure that all your passwords are unique? Do you encrypt all confidential information that you store on your computer and send from it? Are you prepared for loss of your computer? Do you have a backup of all the information in a separate place? Do you destroy unwanted information so it cannot be recovered? Do you know how to access or send the information in a way that nobody can spy on you?[7]
BEING WITNESSES OR HAVING KEY INFORMATION	Are members of your group key witnesses to raise charges against a powerful actor? Do you have relevant and unique information for a given case or process?
HAVING COHERENT AND ACCEPTABLE EXPLANATION ABOUT YOUR WORK AND AIMS	Do you have a clear, sustainable and coherent explanation of your work and objectives? Is this explanation acceptable, or at least tolerated, by most/all stakeholders (specially armed ones)? Are all members of the group able to provide this explanation when requested?

contd. over

COMPONENTS OF VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS VULNERABILITIES OR CAPACITIES
SOCIAL AND ORGANISATIONAL COMPONENTS	
EXISTENCE OF A GROUP STRUCTURE	Is the group structured or organised in any way? Does this structure provide an acceptable level of cohesiveness for the group, including a structure for information sharing; i.e. who knows what in the group?
ABILITY TO MAKE JOINT DECISIONS	Does the group's structure reflect particular interests or represent the whole group (extent of membership)? Are the main responsibilities carried out and decision-making done by only one or a few people? Are back-up systems in place for decision-making and responsibilities? To what extent is decision-making and implementation participatory? Does the group's structure allow for: a) joint decision-making and implementation, b) discussing issues together, c) regular and effective meetings, d) none of the above?
SECURITY PLANS AND PROCEDURES	Are security rules and procedures in place? Is there a broad understanding and ownership of security procedures? Do people follow the security rules?
SECURITY MANAGEMENT OUTSIDE OF WORK (FAMILY AND FREE TIME)	How do you manage your time outside of work (family and free time)? Alcohol and drug use represent great vulnerabilities. Relationships can also result in vulnerabilities (as well as strengths).

COMPONENTS OF VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS VULNERABILITIES OR CAPACITIES
WORKING CONDITIONS	Are there proper work contracts for everyone? Is there access to emergency funds? Insurances?
RECRUITING PEOPLE	Do you have proper procedures for recruiting personnel or collaborators or members? Do you have a specific security approach for your occasional volunteers (such as students, for example) or visitors to your organisation?
WORKING WITH PEOPLE OR WITH INTERFACE ORGANISATIONS	Is your work done directly with people? Do you know these people well? Do you work with an organisation as an interface for your work with people?
TAKING CARE OF WITNESSES OR VICTIMS YOU WORK WITH	Do you assess the risk of victims and witnesses, etc., when you are working on specific cases? Do you have specific security measures when you meet them or when they come to your office? If they receive threats, how do you react?
NEIGHBOURHOOD AND SOCIAL SURROUNDINGS	Are defenders socially well integrated in the local area? Do some social groups see your work as good or harmful? Are you surrounded by potentially hostile people (neighbours as informers, for example)?
MOBILISATION CAPACITY	Are you able to mobilise people for public activities?

contd. over

COMPONENTS OF VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS VULNERABILITIES OR CAPACITIES
PSYCHOLOGICAL COMPONENTS (GROUPS/INDIVIDUALS)	
ABILITY TO MANAGE STRESS AND FEAR	Do key individuals, or the group as a whole, feel confident about their work? Do people clearly express feelings of unity and joint purpose (in both words and action)? Are stress levels undermining good communications and interpersonal relationships?
DEEP FEELINGS OF PESSIMISM OR PERSECUTION	Are feelings of depression and loss of hope being clearly expressed (in both words and action)?
WORK RESOURCES	
ABILITY TO UNDERSTAND WORK CONTEXT AND RISK	Do you have access to accurate information about your working environment, other stakeholders and their interests? Are you able to process that information and get an understanding of threats, vulnerabilities and capacities?
ORGANISATIONAL	
ABILITY TO DEFINE ACTION PLANS	Can you define and, in particular. implement action plans? Are there previous examples of this?
ABILITY TO OBTAIN ADVICE FROM WELL INFORMED SOURCES	Can you obtain reliable advice? From the right sources? Can the group make independent choices about which sources to use? Do you have access to particular organisations or membership status that enhances your protection capacities?

COMPONENTS OF VULNERABILITIES AND CAPACITIES	INFORMATION NEEDED TO ASSESS VULNERABILITIES OR CAPACITIES
PEOPLE AND AMOUNT OF WORK	Do the people or personnel available match the amount of work needed? Can you plan field visits in teams (at least two people)?
FINANCIAL RESOURCES	Do you have enough financial resources for your security? Can you manage cash in a safe way?
KNOWLEDGE ABOUT LANGUAGES AND AREAS	Do you know the languages needed for the work in this area? Do you know the area properly? (roads, villages, public phones, health centres, etc.)
ACCESS TO NATIONAL & INTERNATIONAL CONTACTS & MEDIA	
ACCESS TO NATIONAL AND INTERNATIONAL NETWORKS	Do you have national and international contacts? To visiting delegations, embassies, other governments, etc.? To community leaders, religious leaders, other people of influence? Can you issue urgent actions via other groups?
ACCESS TO MEDIA AND ABILITY TO OBTAIN RESULTS FROM THEM	Do you have access to media (national, international)? To other media (independent media)? Do you know how to manage media relations properly?

NOTES