TRAVEL GUIDANCE AND PROCEDURE

2024

CONTENTS

INTRODUCTION

Travelling internationally will always present additional challenges depending on the destination, the travellers experience and profile, the activities conducted, the level of awareness of safety and security triggers, cultural background, and prevalent and emerging safety and security threats. Associated risk can be largely mitigated through robust preparation and establishing and maintaining situational awareness to avoid unnecessary exposure to risk.

This procedure acts as a checklist and guide for travellers and should be used by them and the GI-TOC's management to assess and mitigate the risk involved in travel and fieldwork.

This procedure details the GI-TOC's travel process for international travel to all destinations, including outlining considerations to ensure inclusive security. It applies to GI-TOC team members, including payrolled staff, remote staff, long-term contractors (when they are paid monthly for a period of 12 months or more) and ad-hoc consultants.

This procedure is designed from the perspective that good travel risk management:

- Should not be onerous, overly bureaucratic, too processed or too prescriptive.
- Should recognize the depth of travel and risk management experience held by the GI-TOC's teams.
- Should provide guidance and allow for discretionary decision-making that can be validated by peer-to-peer and management support structures.
- Should be applicable to all international travel despite the different ways in which the GI-TOC's teams travel and the varied activities they engage in.

INCLUSIVE TRAVEL SECURITY

The profile of an individual, their work activities and the context in which they travel can all contribute to their increased exposure to risk. In recognition of this:

- When choosing who should go on a trip, it is important to think through how potential traveller profiles interact with the destination's localized factors, like religion, ethnicity and language. This ensures that the organization gains a nuanced understanding of local dynamics and does not deploy anyone who would be significantly exposed to risk because of localized contextual factors.
- Once a traveller is selected, the organization can then identify, assess and mitigate individual, organizational and contextual risks using the table below. The inclusive security and increased exposure travel guidelines and targeted questions in the Travel registration and tracking form and the Risk and contingency mission planner, as well as relevant safety and security training, will support this process.
- Finally, travellers and managers can escalate the trip risk level if they feel there is an increased exposure to risk because of profile, activities or context.

The following table identifies some examples of factors that can result in an increased exposure to risk:

| Individual	Organizational	Contextual
- Age - Sex and gender - Sexual orientation, gender identity gender expression - Differently abled - Physical/mental health status - Physical appearance and clothing - Trauma history and/or previous history of being involved in security incidents - Nationality/national origin - Ethnicity - Religion - Marital/partnership status - Education status - Socio-economic status - Attitudes and behaviors - Political membership/affiliation/activity - Previous professional experience - Previous or current employers	- Seniority/hierarchical position - Role/responsibilities - Contract type - Contract duration - Travel obligations - Accommodation - Creating, receiving and sharing sensitive information - Interactions with vulnerable communities (type and frequency) - Relationship with external actors - The GI-TOC's culture and mission	- Legal (national laws and their enforcement, including lack of protections) - Rural, urban, regional differences - Social and cultural beliefs and practices - Religious and other beliefs and practices - Level of acceptance for the GI-TOC's work from various stakeholders, contextual actors and the security environment

TRIP RISK LEVELS

Using a trip risk level tool, we categorize trips as **VERY LOW** , **LOW** , **MEDIUM** , **HIGH** or **VERY HIGH** . The highest risk score, for any given factor, dictates the trip risk level. When the trip is to multiple destinations, we adopt the highest trip risk level for all of the destinations. This ensures that we put in place risk-appropriate mitigation measures. All trips follow the same travel process. However, there are different guidelines that apply based on the trip risk level.

We recognize that there may be circumstances where travellers do not wish to openly share their profile characteristics (for example if those include sexual orientation, gender identity or gender expression). As such, any traveller may escalate the trip risk level (without needing to provide a reason) to ensure that a higher level of travel guidelines is implemented. Conversely, the supervisor can escalate the trip risk level if a manager feels that a traveller has an increased exposure to risk because of their profile, their work with the organization, or the context that they are travelling to.

TRIP PROCESS

To aid understanding, the diagram below is used to represent the trip process. Timings used throughout this procedure are presented as an ideal minimum and only apply to **HIGH** or **VERY HIGH** trip risk levels. 'You' refers to the traveller(s).

Notify → Apply guidelines → Consent and approval → Confirm → Travel → Return
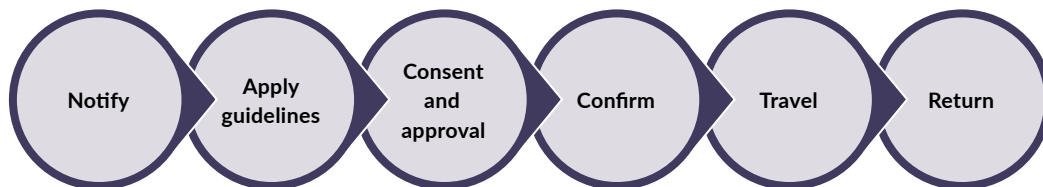
Notify

Once you have completed the trip risk level tool, notify your supervisor of your intended trip. For **HIGH** or **VERY HIGH** trip risk levels this should ideally be four weeks before your departure.

Apply guidelines

Read the trip guidance and ensure that the relevant guidance is considered and applied. For **HIGH** or **VERY HIGH** trip risk levels this should ideally be three weeks before your departure.

Consent and approval

Using the **Travel registration and tracking form** (for `VERY LOW`, `LOW` and `MEDIUM` trip risk levels) or the **Risk and contingency mission planner** (for `HIGH` or `VERY HIGH` trip risk levels) either consent or decline to the trip based on the risk involved and ask your manager to also approve or decline the trip. For `HIGH` or `VERY HIGH` trip risk levels, this should ideally be three weeks before your departure.

Risk approver	
Very low, low and medium trip risk levels	**High and very high trip risk levels**
Manager/Project manager	Director or deputy director

If the residual risk involved in your trip is assessed as above the GI-TOC's risk appetite, the director or deputy director will need to provide the risk approval, regardless of the trip risk level.

Confirm

Once risk approval has been given, confirm your travel arrangements with the travel management company, accommodation provider and relevant others (transport providers, fixers, security providers, etc.). For `HIGH` or `VERY HIGH` trip risk levels, this should ideally be two weeks before your departure.

Travel

During your trip, inform your tether immediately and when safe to do so if you are affected by an incident, near-miss incident, or witness an incident that has caused or has the potential to cause harm to yourself, relevant others or the GI-TOC. In addition, check in with your tether as indicated below and following the tether guidance.

Tether check-in frequency		
Very low and low trip risk levels	**Medium trip risk levels**	**High and very high trip risk levels**
Within 24 hours of arrival at any new destination On any change of itinerary or contact information On arrival to the place of origin AND		
As above	Once per day	Twice per day and at an agreed frequency when on road movements and before and after any sensitive activities (e.g., interviews)

If you miss a check-in, the following loss of contact protocol will be followed:

Loss of contact protocol			
Action taken	**Very low and low trip risk levels**	**Medium trip risk levels**	**High and very high trip risk levels**
▪ Tether continues to attempt check-in with the traveller and tries to trace the traveller through relevant contacts. ▪ Tether informs manager.	6 hours	4 hours	3 hours
▪ Tether continues to attempt check-in with the traveller and tries to trace the traveller through other relevant contacts. ▪ Manager informs director or deputy director. ▪ Critical incident management team activation is considered.	9 hours	8 hours	6 hours
▪ Tether continues to attempt to check in with the traveller and tries to trace the traveller through further contacts. ▪ Critical incident management team automatically activated. ▪ Insurers are informed. ▪ Family liaison officer informs traveller's emergency contact (if not previously informed).	14 hours	18 hours	12 hours

The actions taken in the loss of contact protocol are to be used when a medical, safety or security incident is suspected. As such, common sense should be exercised. For example, if the traveller(s) have not made contact because of known flight delays, there may not be a need to inform the traveller(s) emergency contact(s) at the times indicated, or at all.

Return

If you are affected by or witness an incident, and are a team member, you:

- Can access appropriate and specialized counseling and psychological support through CiC's well-being employee assistance programme. Please see the Operations manual for further information.
- May need to participate in an incident review meeting.

TRIP CHECKLISTS

Below are two checklists for travellers to follow before and during their trip. Relevant points are linked to further guidance provided in this document.

Pre-trip checklist

All trips	- Complete travel registration and tracking form (for low risk and medium risk trips). - Update your next of kin/emergency contacts, if required. - Ensure that you have appropriate permission to enter the destination(s) and your travel documents meet the requirements. - Conduct your own research around the destination(s). - Consider inclusive security and increased exposure. - Conduct first aid training and organize a first aid kit. - Consider medical precautions and responses. Ensure vaccinations in line with national/international health recommendations. - Select suitable accommodation options. - Set-up equipment, including wiping/cleaning, confirming GSM coverage and considering satellite and tracking devices. - Brief your tether, agree check-ins and communicate your intended itinerary. - Brief your home contact and communicate your intended itinerary. - Register your trip with the GI-TOC's insurer. - Confirm your travel itinerary and share it with your tether and your home contact. - Ensure that you have access to emergency money.
Medium trip risk levels	As per all trips and **in addition**: - Complete hostile environment awareness training. - Procure and set up a tracking device. - Identify alternate options for access to/exit from your destination(s). - Establish communication with embassy/diplomatic mission in country or in adjacent country.
High and very high trip risk levels	As per all trips and medium-risk trips, and **in addition**: - Request a specialist report (from the GI-TOC's insurers or a security provider) that includes an updated threat or risk assessment specific to the area(s) where you will travel to within your destination(s). - Discuss and develop your travel and evacuation plans with a security provider, focusing on pick–up points, transportation methods, accommodation, security guidelines, communications, extraction options and incident contingencies. - Consider using/arranging a fixer. - Consider using/arranging a security provider for close protection services. - Complete a proof of life form. - Complete the risk and contingency mission planner and discuss the completed form with either the director or deputy director. - Book airport transfers and in-country ground transportation with trusted/recommended/known contacts. - Procure contextually appropriate clothing (if required).

During-trip checklist

All trips	■ Test your communications equipment to ensure it is functioning. ■ Ensure your tether communications are functioning and check in as agreed. ■ Maintain communication with your home contact. ■ Carry copies of your relevant documentation, e.g., passport, invitation letters, pre-travel authorization/visas. ■ Familiarize yourself with the immediate surroundings, check the safety and security of your accommodation and think about access and exit routes, in case of an incident. ■ Complete your activities considering your research and any specialist advice received. ■ Remain low-profile and avoid presenting yourself as a valuable target. Do not display wealth, expensive jewelry, accessories or visible cash. ■ Tune in to local and international news to understand any travel disruptions or security incidents. ■ Communicate your travel and movements on a need-to-know basis. Do not post them on social media. ■ Avoid protests, mass gatherings and major public events. ■ Report any incidents, near misses or concerns to your tether or manager.
Medium trip risk levels	As per all trips and **in addition**: ■ Test your tracking device is working. ■ Confirm presence with respective diplomatic mission. ■ Do not communicate plans too far in advance and be prepared to change them. ■ Limit unnecessary movements and travel as light as possible. ■ Avoid establishing routines – vary timings and routes. ■ Locate public transport stations/stops/ranks for quick exit situations. ■ Prepare a grab bag with essential documents and equipment that could be required in an emergency.
High and very high trip risk levels	As per all trips and medium risk trips, and **in addition**: ■ Meet with your fixer/security provider as soon as possible and request an on-arrival briefing and situation update. ■ Activate your tracking device and other comms equipment. ■ Before attending sensitive/high-risk meetings, have your fixer/security provider conduct reconnaissance of the location and brief you on routes and alternate routes to and from the location, access to the venue, routes in and out in case of an incident and places to take cover in case of attack. ■ Respect agreed red zones and do not move or stay out in the hours of darkness.

TRIP GUIDANCE

Permission to enter and travel documents

Ensure that you have appropriate permission to enter the destination(s). This can range from nothing to invitation letters, pre-travel authorization and visas. Remember that entry requirements can also relate to the expiry date of your passport and the number of blank pages in your passport. Be aware that some countries will immediately deny entry if the presence of an entry stamp from other specific countries is present in your passport. You may wish to consider having a new passport issued if travel to previous countries may be seen as contentious by authorities in your destination(s).

Ensure that you have multiple sets of good quality copies of your essential documents to ensure redundancy if original travel documents are damaged/lost/stolen or retained. Copies of essential documents can also be uploaded to a secure cloud to be used when required. Your passport, visa, entry stamp page, travel tickets, national identity card, professional identity card, driving licence and immunization record are some of the essential documents that you may want to consider copying. Depending on your trip, it may be a good idea to have the copies waterproofed to make them more resistant to wear and tear. Finally, consider storing copies in different bags/locations so that the redundancy is enhanced and always present the documents that are easiest to replace.

Conduct your own research around your destination(s)

You should develop an understanding of the location(s) that you are visiting before your trip. Remember you should identify and research likely periods of increased risk including elections and national holidays. The level of research that you need to conduct should be proportionate to the trip risk level.

The GI-TOC's insurance provides access to specialists who can provide destination specific advice or are likely to have relationships with other trusted security and service providers operating in the destination. This will allow them to provide detailed analysis, including a detailed threat or risk assessment, if required.

There are many online open-source resources that can support your research. A good starting point is to download a country of interest report that will help you with your situational awareness and understanding of the local context, from the GI-TOC's insurer's website (https://www.garda.com/crisis24).

In addition, the following websites also provide a reliable source of information:

- UK FCDO's Foreign Travel Advice website (https://www.gov.uk/foreign-travel-advice).
- US Department of State website (https://www.state.gov/).
- Australia's Foreign Affairs Smart Traveller website (https://www.smartraveller.gov.au/).
- OSAC's Country Safety Reports (https://www.osac.gov/Content/Browse/Report?subContentTypes=Country%20Security%20Report).
- INSO's NGO Safety Reports (https://ngosafety.org/analysis-reports/).
- Civicus Monitor's Civic Space Ratings (https://monitor.civicus.org).
- Reporters Without Borders Country Ranking (https://rsf.org/en/ranking).

These open-source websites provide a very good understanding of the general situation in the country of interest and will cover all aspects of travel, from entry requirements and recommended immunization to prevalent safety and security conditions.

Localized information can be obtained through local media websites and contacts who may be familiar with your destination(s) such as security providers, humanitarian workers, journalists and locals. Fixers and/or paid informants can also be hired to develop situational awareness. This will give the traveller a better understanding of the context. Depending on the trip risk level, the research should cover key power brokers, areas of influence, key issues at play, communicated and planned disruption to services and the general safety and security situation. Research based on multiple sources will provide a more balanced understanding.

The aim of this research is to establish a good understanding of the context and the initial support one can expect in the case of a safety or security incident. Research areas could include:

- Main threats and concerns.
- General level of risk exposure in your destination(s).
- Cultural norms and associated legal proceedings and outcomes.
- Own country representation in country[1] (Consulate/Embassy location and emergency numbers, establish contact before departure).
- Status of security forces, including distinguishing insignia and uniforms.
- Status of emergency services and respective telephone numbers.
- Status of main entry points (airports, land and sea) and alternates.

If you feel that the information you have is not sufficient, there are a number of security providers that can provide detailed risk analysis and associated services, such as crises response and kidnap and ransom plans.

Consider inclusive security and increased exposure

It is vital that you consider how your profile intersects with the context of your destination(s) before your trip so that you can understand any potential increased exposure to risk. Use the inclusive travel security table to support your identification of factors that could result in your increased exposure to risk.

Remember that we recognize that there may be circumstances where travellers do not wish to openly share their profile characteristics (for example, sexual orientation, gender identity or gender expression). As such, any traveller may escalate the trip risk level (without needing to provide a reason) to ensure that a higher level of travel guidelines is implemented.

There are many online open-source resources that can support your analysis and the development of mitigation measures. Below are some useful starting points for LGBTQI+, female and differently abled travellers.

LGBTQI+ traveller information
- US State Department's LGBTQI+ Travelers Guide (https://travel.state.gov/content/travel/en/international-travel/before-you-go/travelers-with-special-considerations/lgbtqi.html).
- UK Government's Lesbian, Gay, Bisexual and Transgender foreign travel advice (https://www.gov.uk/guidance/lesbian-gay-bisexual-and-transgender-foreign-travel-advice).
- ILGA's Sexual Orientation Laws Map (https://ilga.org/maps-sexual-orientation-laws).
- Stonewalls' LGBT Global Workplace Country Briefings (https://www.stonewall.org.uk/resources-creating-lgbtq-inclusive-workplace/resources-global-lgbtq-workplace-inclusion/global-workplace-briefings).
- IGLTA's LGBTQ+ Safety Guide (https://www.iglta.org/destinations/travel-guides/lgbtq-safety-guide/).
- Equaldex's Equality Indexes for homosexuality, gay marriage, censorship, changing gender, non-binary gender recognition and more (https://www.equaldex.com/).

Female traveller information

- US State Department's Women Travelers Guide (https://travel.state.gov/content/travel/en/international-travel/before-you-go/travelers-with-special-considerations/women-travelers.html).
- Caroline's Rainbow Foundation's Female Travel Tips (https://www.carolinesrainbowfoundation.org/female-travel-advice/).
- UK Government's Advice for Women Traveling Abroad (https://www.gov.uk/guidance/advice-for-women-travelling-abroad).
- UN Women's Global Database on Violence against Women (https://evaw-global-database.unwomen.org/en).

Differently abled traveller information

- US State Department's Travelers with Disabilities Guide (https://travel.state.gov/content/travel/en/international-travel/before-you-go/travelers-with-special-considerations/traveling-with-disabilties.html).
- UK Government's Disability and Travel Abroad Guide (https://www.gov.uk/government/publications/disabled-travellers).

When developing mitigation measures, remember that profile-based mitigation measures often go beyond traditional physical security mitigation measures. For example, travelling in groups, booking an aisle seat on a flight, staying in areas where there are no rowdy bars, not using your title ('Miss', 'Ms' or 'Mrs') when booking accommodation, not sharing details of your trip on social media, not leaving drinks unattended, staying on an accessible floor at the hotel.

It is also important to share your profile-based mitigation measures with fellow travellers and your tether (where you are comfortable to do so), because this will increase their understanding of any increased exposure considerations and enable them to take an active part in mitigation measures.

Consider medical precautions and responses

You should ensure that you have considered and prepared for the potential health impacts of visiting the destination(s). This includes ensuring that you have the correct and up-to-date vaccinations, prescriptions (including eyeglasses or corrective lenses, where relevant), medications, prophylaxis, contact lenses/fluids and general health and hygiene products (including female sanitary products, where relevant).

Different countries have different laws around travelling with prescription drugs, and different positions on what drugs are defined as prescription drugs. If you are travelling with medications, you should check if they are legal in the destination(s) that you are travelling to and travel with a copy of the prescription for each prescription drug that you bring with you, ensuring it is issued, signed (and ideally stamped) by a qualified medical practitioner. This may seem to be excessive, but travellers are sometimes imprisoned for carrying medications that are illegal in their destination (but legal in their country of residence). Also, consider if you have any pre-existing medical conditions, especially those that may require special treatment or emergency care, because they are sometimes not included in the GI-TOC's insurance policies.

Before your trip you should follow the recommended immunization programme. The national health authorities will be able to advise on the immunization requirements. Failing this, the World

Health Organization (http:// www.who.int/en/) and the Centers for Disease Control and Prevention (https://wwwnc.cdc.gov/travel/) provide useful resources. Dental and physical health may need to be assessed and confirmed before your trip as the quality of services may be poor or unavailable altogether.

Especially for <mark>HIGH</mark> or <mark>VERY HIGH</mark> trip risk levels, we recommend that you establish the location, services, required documentation and opening hours of medical facilities within the GI-TOC's insurer's network and confirm if these medical facilities have direct billing arrangements in place (with the GI-TOC's insurer) or demand payment in advance of any diagnosis or treatment.

Select suitable accommodation options

The requirement for accommodation will depend on the tasks and activities included in the deployment. Premises that have a secure compound and are access controlled are recommended. If this is not possible, consider the following:

- Does the accommodation have a definable perimeter wall?
- Does the accommodation provide an appropriate level of security?
- Are there multiple access/exit points including working fire escape exits?
- Does the room have a secure door (lockable from the inside)?

Set up equipment

General equipment

Equipment requirements will vary depending on the required activities and trip risk level. Keep the amount of equipment to the working minimum. Your destination research should indicate the required equipment and availability. Remember that the flashier the equipment, the more attention it will attract. In some countries, photographic equipment that would generally be considered innocuous can attract the attention of border forces, police or intelligence agencies.

Satellite phones

Although most countries will have workable GSM networks, expect difficulties in connectivity once you move to more rural areas. If connectivity is likely to be an issue and of importance, consider taking a satellite phone to ensure continuity of communication. There are several innovative solutions on the market such as sat-sleeves[2] that turn your iPhone or Android device into a satellite phone, allowing you to use your favourite apps and have access to in-country required contacts. There are also Push to Talk (PTT)[3] solutions that allow for complete communication via a satellite network at speeds comparable to GSM networks. Before selecting a device or service provider, always ensure that satellite coverage is available in the destination(s) you are travelling to.

Electronic devices and communications

Ideally you should travel with smartphones/tablets/laptops that can be ditched, if required. Before your trip, 'wipe' or 'clean' your devices to remove any data or contacts that are not required for your work in country. The following are precautionary measures that should become basic practice for all travellers whose electronic devices could be targeted for surveillance or information:

- Where possible, always use communication tools that allow end-to-end encryption.
- Remember that even though you may secure information, connections and communications, others (including partners, grantees and fellows) may not be doing the same.
- As such, always work on the assumption that your electronic communication is not secure and may be monitored. This will require you to think through what is necessary (and unnecessary) to communicate, ensure that you only communicate necessary information and do so in a way that would not likely expose those involved.
- Use strong and unique passwords. Avoid using the same password for multiple applications and/or devices.
- Use two factor authentication (where available) on all your accounts and apps. We recommend using an authenticator app to do this, as opposed to SMS systems tied to your normal phone number as this may not work in your destination(s).
- Consider using a VPN and check the destination's laws regarding their use.
- Always keep your devices as clean as possible to ensure their continued functionality.
- Store fieldwork data on a physical external hard drive and/or encrypted cloud storage system.
- During sensitive fieldwork, particularly for **HIGH** or **VERY HIGH** trip risk levels, make sure you delete any sensitive and/or compromising data from your electronic devices, especially before entering any airports or crossing land borders.

Tracking devices

There are several tracking devices that are available on the market. Most will use GSM, satellite or a combination of both. The advantage of having such a device, either as a standalone or through a phone, is that your next of kin and tether can keep track of your whereabouts. The disadvantage is that the device could attract unwarranted attention, especially when at check points and border crossings or when engaging with people that may want to keep their location unknown. Using a tracking device will be a judgement call and must be considered in light of the pros and cons that such a device will provide.

The pros:

- Tracking of your location that can be set at regular intervals.
- Tracking can be received by your next of kin or tether, anywhere in the world.
- Emergency button activation in the case of an incident.
- Ability to send emergency messages even when cell phone networks are down.

The cons:

- Most devices will need to be in a position that allows a line of sight to the sky.
- May be seen as an attempt to track the whereabouts of third parties/check points etc.
- May be illegal to import and use in specific countries.
- May increase the risk of reprisals from aggressors (e.g., kidnappers) if found on body.

Brief your tether

Regardless of the trip risk level, you should designate one trusted person (who works for the GI-TOC) to act as your 'tether'. This person should have a copy of your itinerary so that they know your planned movements and trip details and can perform the agreed check-ins with you. The frequency of check-ins depends on the trip risk level and the planned activities. Ultimately, you should agree a frequency that is both relevant and achievable for your trip. For trips that have sensitive or particularly risk-exposing activities (e.g., some fieldwork interviews) it is recommended to agree and conduct check-ins before and after these specific activities.

When agreeing the check-in method with your tether, Signal (https://signal.org/download/) is recommended because every Signal message and call are end-to-end encrypted, and (unlike WhatsApp) it is not known to be vulnerable to Pegasus spyware. However, available platforms and connectivity may dictate the use of other similar apps or satellite communications. In situations where there is a heightened abduction risk, it is also advisable to carry a tracking device that feeds information on your movements (and any emergency alerts you submit) to a platform accessible to your tether.

The level of detail that is shared during check-ins should also be pre-agreed with your tether. There may be confidentiality constraints on the sort of information that can be relayed. However, in scenarios where there is an elevated risk of abduction or other critical incidents, your tether should have as much information as possible and be informed of any changes to your plans. In these scenarios, as a minimum, you should also establish prowords/codewords for core messages including 'all ok'; 'minor difficulty – a delay/change of plan, but nothing to worry about'; 'emergency – support required'.

Remember that having too structured or too ridged check-ins could draw attention from anyone conducting surveillance. As such, make the check-ins as informal as possible so that they look like a normal conversation between friends. This will also help to place less stress on you and the tether, while allowing for purposeful contact. For the same reasons, we do not recommend using calendars to schedule check-ins.

If your tether does not hear from you within the times indicated in the loss of contact protocol above, they will escalate this accordingly so that the GI-TOC can take the indicated actions, which could include activating the critical incident management team.

Brief your home contact

Before your trip, you should establish and brief a home contact. Although this can be multiple points of contact, for ease of communication, we recommend a single point of contact. Your home contact can also be your immediate next of kin, although we encourage you to think about who the most appropriate person is for your individual circumstances. If your home contact is not your immediate next of kin, then they should be given the contact details of your immediate next of kin.

Make sure that you provide your home contact with your itinerary and contact telephone numbers.

Register with the GI-TOC's insurer

Insurance covering team members and consultants travelling on behalf of the GI-TOC for business is provided, including for high-risk locations. Before your trip, it is mandatory that you register with the

GI-TOC's insurer so that you can get emergency medical care and evacuation support, if required. Guidance on how to register can be found on the Operation manual, under Insurance. Registration also provides access to useful information such as the policy's key features and country of interest reports. Ensure you carry the details of the policy with you when you travel.

Ensure you have access to emergency money

We recommend that you travel with some emergency money, ideally in the local currency, that can be used to fund unexpected situations and is in addition to any other funds. Travelling with the equivalent of €50 to €100 is sufficient for **VERY LOW**, **LOW** and **MEDIUM** trip risk levels. The equivalent of €300 is sufficient for **HIGH** or **VERY HIGH** trip risk levels. It is advisable to distribute large sums of money in different places on your person and in your luggage.

Complete hostile environment awareness training

Training is a core part of preparation. Through training you can develop the mindset and skillset to maintain awareness of your surroundings, understanding how to mitigate threats and respond to potential incidents. Furthermore, when travelling to countries where insecurity prevails, training in trauma first aid, weapons ammunition and explosives awareness, checkpoint negotiations and incident response may well be lifesaving.

Hostile Environment Awareness Training (HEAT) should be considered, and may sometimes be mandatory, depending on the types of threats involved in your trip. HEAT will expose participants to theoretical principles and practical exercises in preparation for deployment to hostile environments. Subjects often covered will include trauma first aid, incident management, basic negotiation and actions on incidents such as illegal arrest and detention, bombings, violent crime, coming under fire, mass-casualty incidents, and encountering unexploded ordnance (UXO).

Consider using a fixer

It may be a good idea, or a requirement, to engage a fixer to support your activities in the field. Try to use internationally recognized fixing agencies or those recommended to you by a trustworthy person. Fixers will help source support and facilitate interactions, including with locals. Always remember that you own the decision-making process and therefore your fixer needs to understand that you must be kept in the loop of all that is happening so that you can make the decisions that are supported by the advice being provided by the fixer.

Consider using a security provider

It may be a good idea, or a requirement, to engage a security provider to supply close protection services. Once again, try to use companies that are internationally recognized or are recommended to you by a trusted person. There are many security providers, but one with local knowledge and experience will be better suited to providing the required level of security without being intrusive. Establish the requirement and ensure that they provide a briefing on the security context and arrangements. Feel free to challenge proposed options, especially those that clash with the GI-TOC's policy position of not using armed deterrence, violence or weapons of any kind.

NOTES

1   When your own country is not represented, inquire about bilateral agreements/other embassies that can provide support.
2   https://www.thuraya.com/en/products-list/legacy/thuraya-satsleeve.
3   https://www.iridium.com/products/iridium-extreme-ptt/.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 600 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net