Missionary Field Security: 1-Hour Essentials

Circumspect
GROUP INCORPORATED

Real-world awareness. Practical tools. Rapid readiness.

Michael C. Burris

Circumspect Group Inc.

Overview

Objective:

Equip missionaries with tools to manage real-world risk, protect family, ministry, information, and stay secure on the field.

What You'll Get Today:

- 4 true case studies
- Top 10 Security Best Practices Handouts
- Missionary-ready checklists
- Tools for communications, security/safety, cyber safety & evacuation

The Lord will Equip YOU for the Role, He Gives YOU!

Circumspect
GROUP INCORPORATED

Why Do We Need Situational Awareness?

- Because of Local Criminals
- Because of Civil Unrest

  (Protests – Labor, Civil, or Political)
- Because of Organized Crime (Enterprise)
- Because of Terrorist
- Because of Other "Religious" Organizations
- Because of State Security Services (Foreign Country)
- Because of Natural Disasters

Situational Awareness: **Staying updated on the conditions and activities in your neighborhood, city, state, and country.**

What is Safe, What is NOT, What Looks Right and What is OUT of place.

What Man-made or Natural Threats could affect my ministry and me personally?

Stay Informed & Alert

- www.state.gov (Alerts & Advisories)
- **SMART traveler Enrollment** (use “in country #)
- Know Your **Regional Security Officer (RSO)**
- CDC Travel Health
- Local Missionaries
- Cyber Alerts: Here are the biggest travel dangers of 2025 - Elliott Report
- www.google.com
- www.tripadvisor.com & Travel Blogs
- www.circumspect.us **(Missionary Support Package)**
- Mission Board Field Representative
- Trusted News Outlets: VOA, BBC, France 24, SkyNews, “The Local”.com
- **Local** (Mayor, Police, Other Expats)

Be A Critical Thinker!!

Circumspect
GROUP INCORPORATED

Top 5 Missionary Security Principles

Principle	Practice
Be Discreet	Don’t overshare locations or ministry work
Be Prepared	Plan for worst-case scenarios
Be Aware	Track local intel & changes
Be Secure	Lock down devices, accounts, info
Be Accountable	Stay in regular contact with your team

The Greatest Security Countermeasure is YOUR Knowledge & Situational Awareness

Circumspect
GROUP INCORPORATED

🧳 Case Study 1: OPSEC Failure – Oversharing Online

📍 Location: Southeast Asia

📝 Scenario:

A missionary couple regularly updated their public blog and Facebook page with prayer requests, including ministry locations, travel schedules, and names of local partners. A local intelligence unit began monitoring them, flagged their activity as foreign interference, and pressured their visa sponsor to cancel their residency. They were quietly expelled within 48 hours.

🎯 Security Failure:

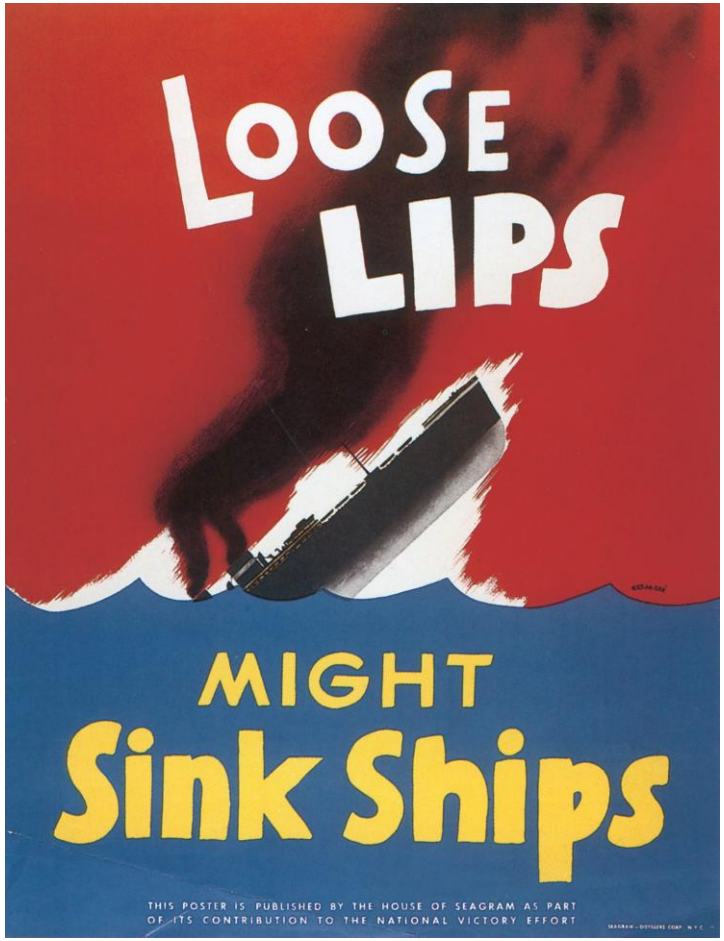
- Public digital footprint compromised operational security.
- Local partners were put at risk due to named association.

✅ Learning Point:

- Avoid sharing *operational details* publicly.
- Use encrypted, invitation-only channels (e.g., Signal, ProtonMail).
- Create a personal OPSEC checklist.

Operations Security

- Protection of your information that can be seen or observed by the public:
  - Time you leave for work
  - Where you work
  - What type work you do
  - Do you Travel
  - Are you Home or Gone
  - Where, What and When do you buy groceries
  - Who is in your Family & What are their habits



Deviation and Variation in your Routine… Is GOOD OPSEC

Operations Security

- Develop a Critical Information List) CIL (Circle of Trust)
- Keep a low Profile
- Be Unpredictable
- Be Aware
- Ensure Unoccupied Facilities (Look Occupied)
- Filter your Social Media
- Control your Trash

CIL

- ✓ **Travel Dates & Locations**
- ✓ **Employee & Visitors Travel Dates**
- ✓ **Physical Security of your Facilities**
- ✓ **Location of High Value Items**
- ✓ **Your Emergency Action Plan**
- ✓ **Vacation Dates**
- ✓ **Times & Routes to Banks, Grocery Store, Church, & School**

Case Study 2: Civil Unrest & Emergency Evacuation

📍 Location: West Africa (2022)

📝 Scenario:

A missionary family found themselves in the capital during a sudden military coup. The airport closed, roads to the embassy were blocked, and their house (in an expatriate neighborhood) became a target for looters. They had no evacuation plan and couldn't reach their local partners for two days.

🎯 Security Failure:

- No pre-planned evacuation route.
- No established crisis communications chain.
- Lack of situational awareness about rising tensions.

✅ Learning Point:

- Always maintain a “go bag” and multiple exit routes.
- Know embassy and host government emergency protocols.
- Use SMS/WhatsApp broadcast lists for updates during outages.

Smart Traveler Enrollment Program (STEP)

Smart Traveler Enrollment Program (STEP)

Are you traveling or living outside the U.S.? STEP is a free service that sends you emails with updates from the local U.S. embassy or consulate. If there's an emergency where you are, it helps us contact you with instructions on what to do.

Why join STEP?

- Get real time updates about health, weather, safety, and security in the country.
- Plan ahead using information from the local U.S. embassy.
- Help the embassy or consulate contact you if there's an emergency like a natural disaster, civil unrest, or a family emergency.

What kind of messages does STEP send?
Currently, STEP sends emails only. STEP can send you several types of information:

- **Routine Messages**: News and updates about the country you picked.
- **Alerts**: Messages about short-term security, terrorism, health, weather, or disaster situations that could impact your travels.
- **Travel Advisories**: We re-evaluate the situation in each country every 6-12 months. Advisories include a simple 1-4 rating system, details about specific risks in the country, and clear steps U.S. citizens should take to stay safe.

Join the Smart Traveler Enrollment Program (STEP)

After you set up your account, you can pick what types of messages you want to get.

Stay in touch during an emergency. Signing up for STEP helps the U.S. embassy get in touch with you if there's an emergency. And, if your family or friends in the U.S. can't reach you with urgent news while you're traveling, we can use the information in STEP to try and contact you.

Become a Smart Traveler Now! STEP is an easy first step to being a smart traveler. You should also always research your destination, and consider additional ways to get safety and security information from the U.S. Department of State, like on social media.

Last Updated: March 5, 2024

Smart Traveler Enrollment Program

About the service

Smart Traveler Enrollment Program (STEP) is a free service to allow U.S. citizens and nationals to enroll their trip abroad so the Department of State can accurately and quickly contact them in case of emergency.

Benefits

- Get real time updates about health, weather, safety, and security in the country.
- Plan ahead using information from the local U.S. embassy.
- Help the embassy or consulate contact you if there's an emergency like a natural disaster, civil unrest, or a family emergency.

Time to complete: 20 minutes

OMB Control No. 1405-0152 | Expiration Date: 06/30/2026

Start

Useful Links

Get help with technical issues on STEP

Search for U.S. Embassies and Consulates

Learn about your destination: Country Information Page and Travel Advisory

Stay Connected: Additional ways to get safety and security information

Before you go see our traveler's checklist

Travelers with Special Considerations

Evacuation Quick Plan Template

Key Info to Know BEFORE You Go:

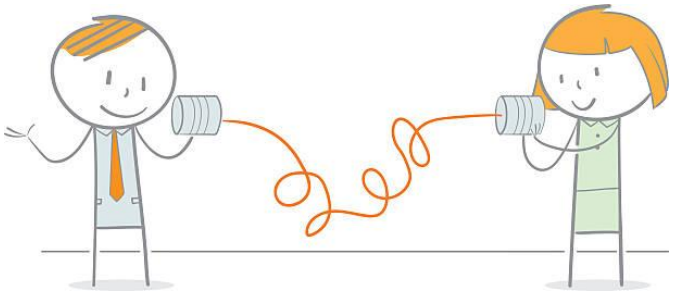
- Safe Meeting Locations (A & B): _____
- Embassy Contact (RSO): _____
- Trusted National Partner: _____
- Evac Routes (A, B, C): _____
- Cash Access Point / Go-Bag Spot: _____
- Home Base Contact (Back Home): _____

💡 *Fill this out. Print it. Keep it safe.*

A **PACE plan** refers to a **Primary, Alternate, Contingency, and Emergency (PACE) communication plan.**

PACE Communication Plan

Communication Tier	Method	Tool/Platform	Point of Contact	Notes
Primary	Voice Call	Local Mobile (Safaricom)	Team Leader (local)	Daily check-ins
Alternate	Internet App	WhatsApp or Signal	Field Security Officer	For low-cost messaging/calls
Contingency	Satellite	Garmin InReach or Iridium GO	Home Church Contact	For poor coverage or outages
Emergency	Physical Evac Alert	Prearranged SMS Blast & Safe Haven Protocol	Per your Mission Board SOP or Circumspect Group Hotline	Trigger evacuation plan



Circumspect
GROUP INCORPORATED

Missionary Security Quick Checklist

Before Deployment / While on Mission:

- ✅ Risk assessment completed
- ✅ Local contact network established
- ✅ Emergency plan and go-bag ready
- ✅ Devices secured (encryption + passwords)
- ✅ Secure comms & social media use plan

Case Study 3: Cybersecurity – Phishing Scam

📍 **Location: Latin America / US Support Base**

📝 **Scenario:**

Hackers gained access to an old email account tied to a missionary. They sent urgent donation requests to the support base and churches, claiming the family was in crisis and needed funds immediately. Several donors wired money to an untraceable international account. The missionary didn't discover it for two weeks.

🎯 **Security Failure:**

- No two-factor authentication (2FA).
- No "fraud warning" system for financial requests.
- Unclear separation between personal and ministry comms.

✅ **Learning Point:**

- Secure all accounts with MFA.
- Notify supporters in advance: "We never request money this way."
- Regularly audit and close unused email and social accounts.

Circumspect
GROUP INCORPORATED

Spot the Phishing Attack

Top 5 Phishing Red Flags:

- 🚩 Weird email addresses
- 🚩 Urgent language (“Send money now!”)
- 🚩 Mismatched URLs
- 🚩 Unfamiliar attachments
- 🚩 Vague greetings (“Dear friend”)

Best Practices:

- ✅ Use secure email (ProtonMail, Tutanota, Signal)
- ✅ Set up 2FA on all accounts
- ✅ Verify donation requests via voice or video

Case Study 4: Compromised Ministry Data

📍 Location: Central Asia

📝 Scenario:

A missionary's laptop was stolen while riding public transit. The device had no password protection, and stored donor lists, ministry contacts, and sensitive discipleship records. Within weeks, several local believers were harassed by authorities — one was detained. Investigators believed the files were accessed and traced.

🎯 Security Failure:

- No encryption or access control on device.
- No backup or remote wipe capability.
- Unprotected sensitive information stored locally.

✅ Learning Point:

- Use full-disk encryption & strong password/PIN.
- Backup data securely and remotely (e.g., cloud or external drive).
- Separate and anonymize sensitive records whenever possible.

Circumspect
GROUP INCORPORATED

Data Protection Basics

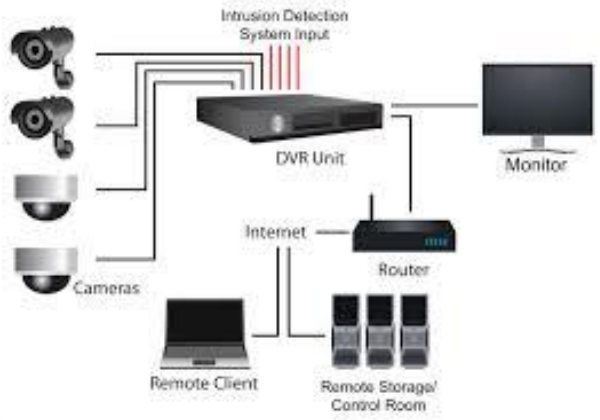
🔐 5 Tips to Protect Your Data:

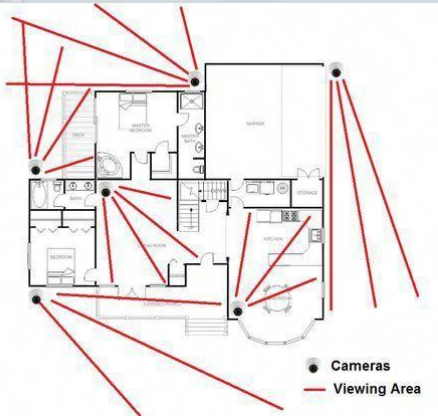
1. Encrypt devices & files
2. Backup to cloud or external drive
3. Keep local contact data off personal devices
4. Use strong passwords or a manager
5. Physically secure all gear (never leave it unattended)

💡 *Enable remote wipe & tracking if possible.*

Physical Security (Secure the Perimeter)

- Traditional Security measures, designed to **Detect, Deny, & Deter** Criminals from acting badly
  - Exterior Illumination
  - CCTV
  - Electronic Intrusion Detection System
  - Fencing
  - Locks
  - ID Cards
  - Obscurants
  - May include Guns, Gates, and Guards





Circumspect
GROUP INCORPORATED

Cyber Security

- Tip #1 - **You are a target to hackers**
- Tip #2 - Keep software up-to-date
- Tip #3 - Avoid Phishing scams - beware of suspicious emails and phone calls
- Tip #4 - Practice good password management
- Tip #5 - Be careful what you click
- Tip #6 - Never leave devices unattended
- Tip #7 - Safeguard Protected Data
- Tip #8 - Use mobile devices safely
- Tip #9 - Install antivirus/anti-malware protection
- Tip #10 - Back up your data

Resources - Notebook

Wrap-Up & Resources

- ✅ Course Notebook (Top 10) Safety & Security Best Practices
- ✅ Security Quick Checklist
- ✅ Fillable Evacuation Plan
- ✅ Phishing Red Flags
- ✅ Secure Comms Best Practices
- ✅ Data Protection Basics
- ✅ Top 5 Missionary Security Principles
- ✅ Case Study Summary Sheet

Thank you for your service and commitment.

Stay Alert. Stay Faithful. Stay Secure.

May God Bless Your Ministry