UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Security Management Operations Manual

Guidelines on Electronic Travel Advisory (eTA App)

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 08 January 2020

TABLE OF CONTENTS

1 INTRODUCTION

1.1 As the United Nations Security Management System (UNSMS) is engaged in the modernization and update of its security communications globally[1], the Electronic Travel Advisory (eTA) is a tool for communicating security information to UNSMS personnel, as well as a means of accounting for UNSMS Personnel.

1.2 **Purpose**: These guidelines articulate roles, responsibilities, and procedures for using the Electronic Travel Advisory (eTA) in security communications and accounting for UNSMS Personnel.

1.3 **Applicability**: These guidelines support all UNSMS security professionals who are engaged in the management or use of the Electronic Travel Advisory (eTA).

2 ELECTRONIC TRAVEL ADVISORY AND SECURITY COMMUNICATIONS

2.1 The eTA is the United Nations Department of Safety and Security (UNDSS)'s security information broadcast and emergency response tool to communicate and account for United Nations Security Management System (UNSMS) personnel[2].

2.2 The eTA, therefore, may be used by security personnel of UNDSS to communicate, account for and obtain reports on all personnel. Each of the other UNSMS organizations can perform the same functions for their own personnel.

2.3 Security professionals must review, propose and manage security communications systems as part of their respective security plans, to communicate security information and respond to emergencies. These measures must be justified through the Security Risk Management (SRM) process, reviewed by the Security Management Team (SMT) and Approved by the Designated Official (DO).

2.3.1 As a result of the SRM process, a Designated Official/SMT should consider to include the use of eTA for all security communications and UNSMS personnel accounting purposes within the Designated Area (DA). As part of this:

2.3.1.1 All UNSMS personnel with UN-issued smartphones should be encouraged to download the eTA App and activate the location services and notification features of their mobile devices.[3]

[1] UNDSS Communique on 29 April 2019: Further Guidance on Security Communications System.
[2] Covered by the UNSMS, as defined in Chapter III of the Security Policy Manual (SPM).
[3] A UN-recognized security information communication tool which receives information from eTA, such as SCAAN, can also be encouraged for use for the same purpose.

2.3.1.2 UNSMS personnel without a UN-issued smartphone should be encouraged to have the eTA App on their personal mobile device to better ensure they have access to available security information.

2.3.1.3 All UNSMS personnel should be encouraged to provide mobile phone numbers that can be reached in their current location, if they have not already done so.

3 CONFIDENTIALITY OF DATA

3.1 All information relating to UNSMS personnel location is confidential and can only be used to respond to declared emergencies involving safety and security of personnel.

3.2 All user location data is only kept for 96 hours; after that time, it is deleted automatically.

4 ROLES AND RESPONSIBILITIES

4.1 The DO and SMT members should encourage all UNSMS personnel under their responsibility who have a UN-issued smartphone, to download the eTA App [4], and to activate its notification and location features so that they can receive security information relevant to their current location.

4.2 If UNSMS personnel do not have a UN-issued, eTA-compatible smartphone, they are encouraged to provide contact information/mobile phone number to their respective Human Resources organizations and/or provide this information in TRIP, both for their assigned duty station and whenever they travel, so that they are able to receive eTA notifications via text message.

4.3 The most senior Security Professional (Principal/Chief/Security Adviser or Chief Security Officer) in the Designated Area is responsible for the establishment, management and monitoring of the eTA Dashboard functions in their Area of Responsibility (AOR).

4.3.1 Additional SOPs to complement these guidelines may be developed by the P/C/SA in conjuction with respective security cell to consider local operational modalities.

4.3.2 The most senior Security Professional in the Designated Area can delegate day-to-day functions of the eTA Dashboard to:

a) Deputy Security Adviser
b) Field Security Coordination Officer
c) Local Security Assistant
d) Mission Security Officer
e) Operators of the Security Communication Centre[5]

[4] This applies to when an eTA-compatible smartphone and corresponding data plan has been issued to personnel.
[5] UNDSS Communique on 29 April 2019: Further Guidance on Security Communications System.

4.4 In the event local UNDSS personnel are incapacitated by a security or hazard event:

4.4.1 The UNDSS 24/7 COMSCEN may use the eTA Dashboard to notify and/or account for staff as directed by the USG or designate.[6]

4.4.2 Members of the security cell at the local level may also be delegated the authority to use the eTA Dashboard for all UNSMS personnel in the relevant SRM Area.

4.5 The following personnel of UNSMS organizations can use the eTA Dashboard functions described herein to provide information to and account for the UNSMS personnel of their respective organizations: [7]

f) Agency HQ Security Focal Point
g) Alternate Agency HQ Security Focal Point
h) Agency CO Security Focal Point
i) Alternate Country Security Focal Point
j) Agency Field Security Adviser
k) Agency HQ Security Focal Point Support Team
l) Agency Local Security Assistant
m) Agency Regional Security Adviser
n) AFP Chief of Security
o) AFP Deputy Chief of Security

4.6 Anyone who is provided authority to view or use any portion of the eTA Dashboard must:

4.6.1 Undergo training available through the UNDSS Learning Management System (LMS) for this use.

4.6.2 Verify that they have read and understood the limitations of eTA use as described in the eTA Legal Framework, as well as acknowledge the limits of the use of eTA functions as outlined in these guidelines. This understanding will be verified as an "in-system" check prior to each person's first use of the eTA Dashboard.

4.6.3 Understand that all activities while using the eTA are recorded in eTA reports and can be reviewed by UNDSS Division of Regional Operations (DRO) Desk Officers and DSOS. This understanding will be verified as part of the eTA course on the LMS.

[6] Designated security personnel can include members of the security cell, who will likely have more immediate information about an event. The COMSCEN is viewed as a back-up for when local capacity is lost.
[7] In many locations, AFP personnel may be acting FSCOs or the adviser to the ASC where there are no UNDSS personnel in a given location and no formal FSCO/SA arrangement. AFPpersonnel who can be delegated authority to use the eTA for their own staff are listed in paragraph 3.7.

4.7 The UNDSS Division of Specialized Operational Support (DSOS) is responsible for monitoring the use of eTA and for identifying and reporting, when necessary, any misuse by any eTA Dashboard user.

4.7.1 Unauthorized use of eTA functionalities by any eTA Dashboard user for purposes other than security-related tasks are prohibited. Misuses of the eTA functions will result in immediate loss of access rights to eTA and their supervisor/ parent organization will be notified.

4.8 Security personnel who experience any technical issues with the eTA should report these immediately through the email <UNDSS.SMSDB@un.org>.

4.9 Users of the eTA who experience trouble with the App should seek technical support via the link provided on the App.

5 HOW THE ELECTRONIC TRAVEL ADVISORY WORKS

5.1 The eTA has two parts, both linked to several UNSMS datasets based in UNSMIN:

5.1.1 **The eTA App** for all UN System personnel. Within the respective SRM Area, eTA App users who download the eTA App and activate its notification as well as location features, can receive eTA notifications, Headcount requests, as well as benefit from the Locate &Assist and Geolocation features, when activated.

5.1.2 **The eTA Dashbord** provides a way for security professionals to interact with eTA App users and UNSMS personnel who have provided their mobile phone numbers to TRIP.

5.2 The information in **Table 1** is provided by UNSMS datasets to the eTA. This data will appear automatically on each eTA App based on location.

Table 1 - UNSMS datasets to the eTA

Data type	Data Source	Data location on App	Responsibility
UN premises	UNSMS Premises Dataset	Homepage "Information" tab	UNDSS country UNSMS personnel or as determined in 3.3
Security Advisory ("Emergency Information")	Travel Advisory	Homepage "Information" tab	UNDSS – country UNSMS personnel or as determined 3.3
Security Clearance status	TRIP	Homepage "My profile" tab	Each UN System personnel
Emergency Contact	Travel Advisory	"Emergency" tab	UNSMS security personnel

5.3 The remainder of these guidelines detail procedures for each of the eTA Dashboard functions which involve near real-time inputs from security professionals.

6 ETA NOTIFICATIONS

6.1 The **Security Notifications** feature of the eTA allows the eTA Dashboard users to send messages directly to UNSMS personnel located in a particular geographical area by either selecting a pre-defined area for a "Quick Notification" or by creating an "Operational Zone" by geofencing an area on the map interface of the eTA Dashboard.

6.1.1 The most senior security professional or designate should select the area to be notified based on operational needs.

6.1.2 These notifications are sent to all eTA end users present in the pre-defined area or Operational Zone as follows:

6.1.2.1 All eTA App users will receive notifications for their current geographic location.

6.1.2.2 UNSMS personnel not using the eTA App, but who have provided their mobile number for their home duty station, will receive notifications for their home duty station even when travelling. For example, if the phone was provided at a parent duty station in New York these personnel will continue to receive notifications for New York even while travelling elsewhere.

6.1.2.3 UNSMS personnel not using the eTA App, but have provided their mobile number in TRIP when they travel will receive notifications for their travel location.

6.2 There are three types of notifications:

6.2.1 **Security Alert:** A security incident has occurred (e.g. a suspicious package);

6.2.2 **Security Warning:** A security situation is imminent (e.g. demonstrations nearby);

6.2.3 **Information Only:** Information provided of an event that could affect personnel operations (e.g. street closure, weather warnings,).

6.3 eTA notifications should be in the language most suited for the area in addition to English.

6.4 Refer to the eTA notifications "How-to" manual for the technical steps involved in sending eTA notifications.

NOTIFICATION QUICK STEPS

1. Determine area where security information is necessary.
2. Select Quick Notification or Operational Zone notification based on determined area.
3. Provide security information and advice via eTA in the language most appropriate for area and English.
4. In areas with unreliable connectivity, send secondary communication by established alternate means.

6.5 When warranted, security communication by UNDSS on behalf of the DO, will be sent to all UNSMS personnel in the impacted area using the eTA Dashboard as the primary means to communicate this security information to UNSMS personnel.

6.5.1 When warranted, security personnel of UNSMS organizations can send security communication to their own personnel using the eTA Dashboard. These security communications can include:

6.5.1.1 Additional information relevant to a single UNSMS organization's personnel that was not included in a security communication delivered by UNDSS.

6.5.1.2 Security information that is only relevant to personnel of an individual UNSMS Organizations.

6.5.1.3 These security communications cannot contradict UNDSS notifications but can provide additional information that is relevant.

6.5.1.4 The DO, Principal/Chief/Security Adviser or Chief Security Officer must be informed of AFP-specific notifications. When available, these notifications will be automatically generated by the system.

7 ETA HEADCOUNT

7.1 There are two ways that eTA can be used to account for UNSMS personnel, an "emergency Headcount," to be used only by UNDSS in the event of a crisis or emergency, and a "Routine Headcount" that can be used by UNDSS and AFPs for routine accounting of UNSMS personnel.

7.1.1 All Headcounts are set to last no longer than 24 hours unless otherwise specified.

7.2 Emergency Headcount

7.2.1 In the event of an emergency/crisis, the most senior security professional of UNDSS in the Designated Area or designate is authorized to use the eTA Headcount feature as one of the primary means to account for UNSMS personnel who could be impacted by an event. This use of the Headcount feature is considered an Emergency Request for Status that is specifically designed to identify and assist those that are impacted by an event.

7.2.2 After following the procedures for Activating a Headcount Zone in eTA and the Headcount "How-to" manual, security professionals responsible for accounting for impacted UNSMS personnel will monitor the status of responses using the Headcount Status interface on the eTA Dashboard or by choosing the appropriate Headcount report as filed in "I'm OK List by Date, Country, and Agency," on UNSMIN.

7.2.3 Actions to be taken by security personnel for each type of response received from UN System personnel via the eTA should include, but are not limited to, the following:

a) In the case of a "NOT OK" response, local procedures known to the security cell personnel as per the security plan for aiding UNSMS personnel should be followed. These can include but are not limited to, activating the Geolocation and/or Locate & Assist features on eTA Dashboard to pinpoint or narrow down on UNSMS personnel location. Every means necessary should be employed to locate UNSMS personnel and assist them.

b) In case of no response during the Headcount, the applicable local procedures known to the security cell personnel as per the security plan of finding/locating the personnel should be followed and assistance provided as required.

c) To ensure all UNSMS personnel that are impacted by an event are assisted as quickly as possible, their respective UNSMS organization security professionals can use the eTA Dashboard to view the Headcount status of their own personnel and coordinate with UNDSS to determine how best to assist.[8]

7.2.4 The monitoring of the Headcount status will be pursued by the most senior UNDSS security professional in the SRM area until a formal deactivation process is determined by the DO.

7.2.5 All information will be maintained in the Data Summary for the use of security managers.

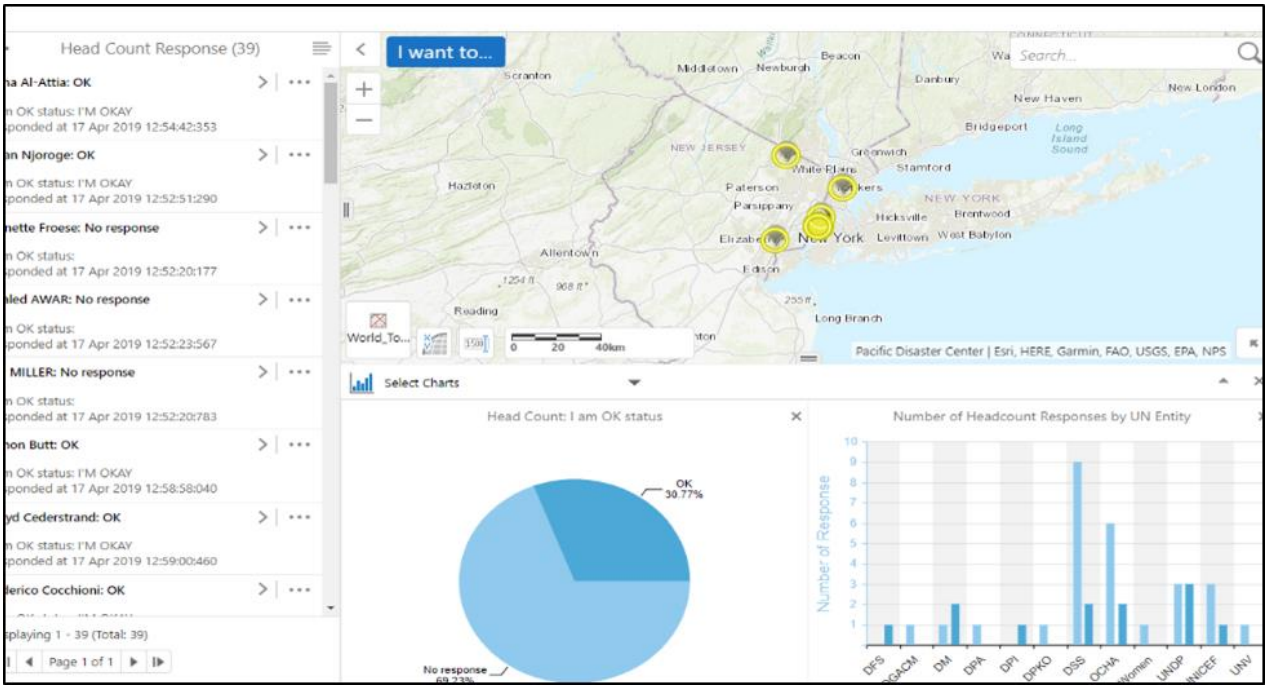
7.2.6 If UNDSS personnel are incapacitated by the emergency/crisis, members of the security cell may be delegated the authority to facilitate the headcount.

[8] Only personnel who have activated the location features for the eTA App will be visible

7.2.7 If UNDSS/ designated security personnel and security cell members in-country are unable to conduct a Headcount, it can be undertaken by the UNDSS 24/7 COMSCEN as directed by the USG or designate. [9]

7.2.8 A representation of an emergency Headcount interface is shown in **Figure 1**

Figure 1 - eTA Headcount interface



7.3 Routine Headcount (functionality still pending as of 6 Feb 2020):

7.3.1 The eTA can be used for routine Headcount procedures/warden system checks by UNDSS and any UNSMS organization, as needed.

7.3.2 These Headcounts should be announced and coordinated within the SMT to ensure no overlap or misuse of the eTA that would hinder its operation as a security management/emergency response tool.

7.3.3 Local SOPs will guide the use of the eTA App for routine Headcount purposes.

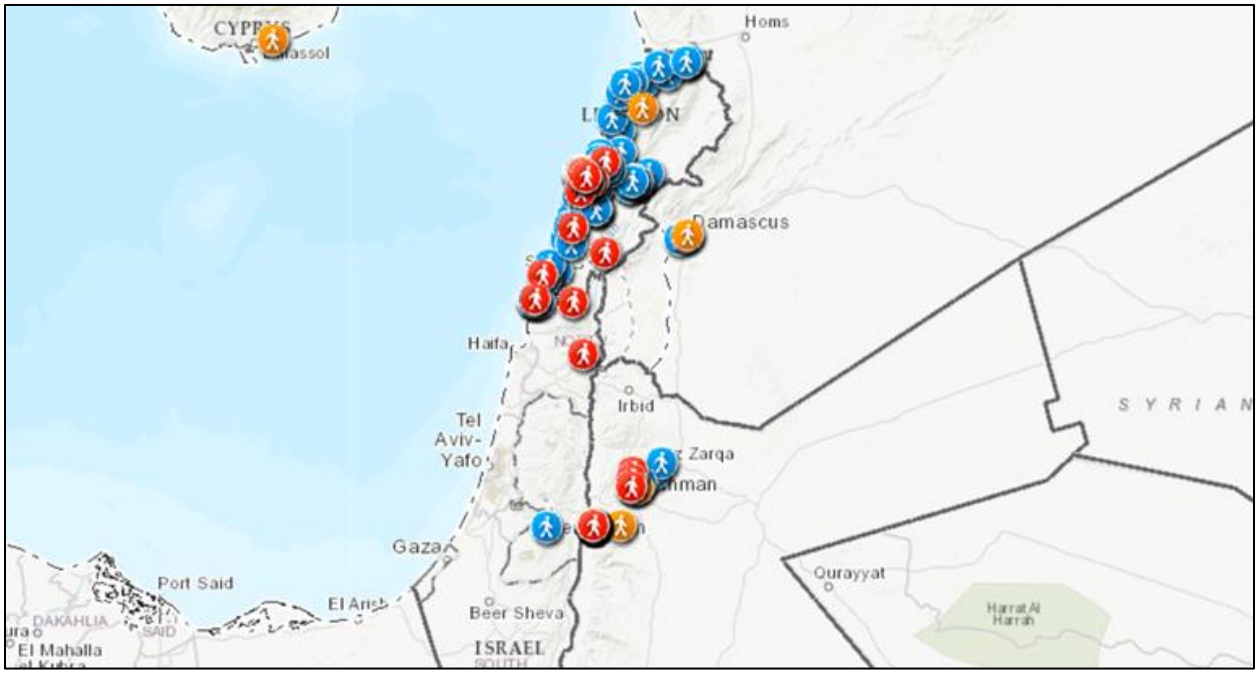
[9] Designated security personnel can include members of the security cell, who will likely have more immediate information about an event. The COMSCEN is viewed as a back-up for when local capacity is lost.

8 ETA GEOLOCATION FEATURE[10]

8.1 The eTA Geolocation feature provides the ability for eTA Dashboard users to see the following information for each eTA App user in the area where the feature is activated:

8.1.1 The last known location, as an icon on the map and as geocoordinates in the user data of UN System personnel. **Figure 2** presents this interface.

Figure 2 - eTA Geolocation interface



8.1.2 Work-related information including functional title, UN employer, work email and phone contact information.

8.1.3 Security clearance status of each individual as represented by the color of the icon[11].

Blue	represents personnel in their assigned duty station
Orange	represents personnel traveling in the area WITH security clearance
Red	represents personnel traveling in the area WITHOUT security clearance

8.2 Only eTA App App users that have the location services for the eTA App activated on their mobile device will be visible on the eTA Dashboard.

[10] The eTA GeoLocation feature refers to the ability of visualizing eTA App users on the eTA Dasboard. The activation of ”location services” on each eTA App user’s phone is an individual decision.
[11] Security clearance is mandatory for official travel and recommended for personal travel.

8.2.1 It is recommended that all UNSMS security professionals encourage personnel to download and activate location and notification services on the eTA App if they have UN-issued smartphones.

8.2.2 Benefits of downloading the eTA App on personal smartphones can also be provided to UNSMS personnel to encourage voluntary download.

8.2.3 UNSMS personnel without the App cannot be geolocated by eTA. These personnel should be informed of a possible reduced ability to assist them in the event of emergency or crisis.

8.3 The default condition of the eTA Geolocation feature should be OFF in every Designated Area.

8.4 Activation of the Geolocation feature is done by clicking on the "eTA Tools – SRM Area Setup" section of the eTA Dashboard and selecting the appropriate SRM Area.

8.5 The eTA Geolocation feature can be turned ON and can remain operational in a Designated Area as an SRM measure approved by the DO/SMT.

8.5.1 This action must be justified by an approved SRM and should stipulate when a review of this necessity is warranted.

8.5.2 UNSMS personnel must be informed of this activation as an SRM measure.

8.5.3 AFP Heads of Office can approve activation of the GeoLocation feature for their own personnel, provided they inform the DO and the P/C/SA of this activation.

8.6 The eTA Geolocation feature can be turned ON for a limited time in the event of an emergency in a Designated Area and the DO informed accordingly:

8.6.1 Emergency situations may include security and safety incidents such as hostage-taking, kidnapping, terrorist attack, and any other natural or manmade incident or disaster that could have harmful impacts on personnel.

8.6.2 This type of limited activation requires that the most senior security professional inform the DO of its activation.

8.6.3 The use of the eTA Geolocation feature for an emergency should be done in conjunction with established Headcount procedures as listed above and as determined locally, if necessary.

8.6.4 The eTA Geolocation feature must be turned OFF when it is determined that all UNSMS personnel that could have been impacted by an event are accounted for and assisted, if required.

8.7 When activated as an SRM measure:

8.7.1 All personnel with UN-issued mobile phones are required to activate the eTA App location services feature on their UN-issued mobile phone or any other UN-issued tool which is capable of receiving notifications from eTA.

8.7.2 All other UNSMS personnel should be encouraged to activate the location services features of the eTA App on their personal smartphone.

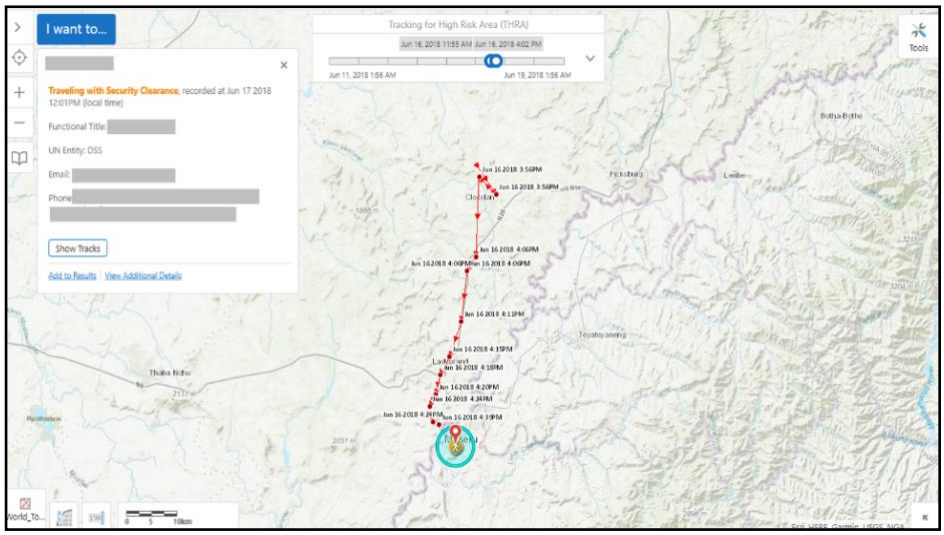
8.7.3 Personnel without smartphones should be notified of the inability for security personnel to know their location in the event of an emergency.

8.8 The activation of the eTA Geolocation feature will be directly managed by the responsible security professional or his/her delegated personnel until directed to deactivate the process by the Designated Official.

9 ETA LOCATE & ASSIST FEATURE

9.1 The Locate & Assist (L&A) feature in the eTA allows for a lasting display of App user Geolocations on the eTA Dashboard, including paths between locations, as presented in Figure 3.

Figure 3 - eTA Locate & Assist Visualization



9.2 Only eTA App users that have the location services for the eTA App activated on their mobile device will be visible on the eTA Dashboard. It is recommended that all UNSMS security professionals encourage personnel to download and activate location and notification services on the eTA App if they have UN-issued smartphones. Benefits of

downloading the eTA App on personal devices can also be provided to UNSMS personnel to encourage voluntary download

9.3 The default condition of the eTA Locate & Assist (L&A) feature is OFF.

9.4 The eTA L&A feature can be turned ON and can remain operational in a Designated Area as an SRM measure approved by the DO/SMT.

9.4.1 This action must be justified by an approved SRM and should stipulate when a review of this necessity is warranted.

9.4.2 UNSMS personnel must be informed of this activation as an SRM measure.

9.4.3 AFP Heads of Office can approve activation of the L&A feature for their own personnel, provided they inform the DO and the P/C/SA of this activation.

9.5 The eTA L&A feature can be turned ON for a limited time in the event of an emergency in a Designated Area and the DO informed accordingly:

9.5.1 Emergency situations may include security and safety incidents such as hostage-taking, kidnapping, terrorist attack, and any other natural or manmade incident or disaster that could have harmful impacts on personnel.

9.5.2 This type of limited activation requires that the most senior security professional inform the DO of its activation.

9.6 The eTA L&A feature must be turned OFF when it is determined it is no longer needed as an SRM measure.

9.7 When activated as an SRM measure:

9.7.1 All personnel with UN-issued mobile phones are required to activate the eTA App's location services feature on their UN-issued mobile phone or any UN-issued tool which is capable of receiving notifications from eTA.

9.7.2 All other UNSMS personnel should be encouraged to activate the features of the eTA App on their personal smartphones.

9.7.3 UNSMS personnel without smartphones should be notified of the inability for security personnel to know their location in the event of an emergency.

9.8 The activation of the eTA L&A feature will be directly managed by the responsible security professional or his/her delegated personnel until directed to deactivate the process by the Designated Official.