Standard Operating Procedure (SOP)
Electronic Travel Advisory (eTA)

1.1. As the United Nations Security Management System is engaged in the modernization and update of its security communications globally[1], the Electronic Travel Advisory (eTA) should become the primary means of communicating security information to UN personnel. All security professionals are to revisit the security communications infrastructure in their area of responsibility to establish eTA as the primary tool of communication, wherever possible. In areas where communications connectivity is limited, and/or mobile communications are not sustainable, other technologies should be used to supplement the eTA.

2. **Purpose**

This Standard Operating Procedure (SOP) articulates roles, responsibilities, and procedures for using the Electronic Travel Advisory (eTA).

3. **Applicability**

This SOP supports all UNDSS security professionals who are engaged in the management or use of eTA.

4. **eTA and security communications**

4.1. The eTA is the Department of Safety and Security's (DSS) primary security information sharing and emergency response tool to communicate with the United Nations Security Management System (UNSMS) personnel[2] except eligible dependents.

4.2. Security professionals must review, propose and manage security communications systems as part of the security plans, to communicate security information and respond to emergencies. These measures must be justified through the SRM process, reviewed by the SMT and approved by the Designated Official. As a result of this process, a Designated Official may make the use of eTA[3] mandatory as a Security Risk Management measure for all UNSMS personnel in their designated area.

[1] Reference UNDSS Communique date 29 April 2019: Further Guidance on Security Communications System (add hyperlink)
[2] Covered by the UNSMS, as defined in Chapter III of the Security Policy Manual (SPM)
[3] "Use" of eTA means that the App's location and notification services are always enabled on personnel's mobile device and carried with them.

4.3. In areas where infrastructure does not adequately support eTA transmission of notifications and/or headcounts, alternate means of communication should be used in addition to eTA to ensure effective and reliable communication with UNSMS personnel.

4.4. Following the adoption of the eTA, UNDSS security professionals will modify and update relevant security communications SOPs and the "Security Communications" portion of their Security Plans.

5. Roles and Responsibilities

5.1. The DO and SMT members must ensure that all UNSMS personnel under their responsibility download the eTA App and activate its notification and location features or provide a mobile phone number to be reachable via the eTA Command Center and are trained to use eTA App.

5.2. The most senior Security Professional - Principal/Chief/Security Adviser or Chief Security Officer (P/C/SA) is responsible for the establishment, management and monitoring of the eTA Command Center functions. They will develop a local SOP to govern its use for providing security information, accounting for staff and supplementing security measures with eTA GeoLocation features, including how to integrate agency security officers in the use of eTA for staff of their own organizations.

5.3. P/C/SA may identify an administrator of the eTA Command Center. They may delegate the authority to send notifications through the eTA to anyone within the security team in the relevant designated area such as. Deputy Security Adviser, Field Security Coordination Officer (FSCO), Local Security Assistant (LSA), Mission Security Officer (DPO/DPA missions), and Operators of the Security Communication Centre[4].

5.4. The 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 Command Center Administrator.

5.5. Anyone who has been provided authority to view or use any portion of the eTA Command Center must undergo training provided through the DSS Learning Management system(LMS) for this use and must certify in writing with DSOS that they have read and understood the limits of eTA use as detailed in the eTA Legal Framework, as well as understand the limits of the use of eTA functions as outlined in these SOP.

[4] Reference UNDSS Communique date 29 April 2019: Further Guidance on Security Communications System (add hyperlink)

5.6. Administrators of the eTA Command Center understand that all actions taken using the eTA are recorded in Command Center Reports and can be reviewed by UNDSS DRO Desk Officers and DSOS. This understanding will be verified as part of the eTA course on LMS and in the "eTA Command Center Administrator Certification Checklist."

5.7. Unauthorized use of eTA functionalities by any eTA Command Center Administrator for purposes other than security-related tasks are prohibited and subject to disciplinary measures. Use of the eTA functions against any individual or group for their gender, race, ethnicity, sexual orientation or other characteristic will result in loss of access rights to eTA.

5.8. Security staff that experience any technical issues with the eTA should report these immediately through the UNDSS.SMSDB@un.org.

5.9. Any App user that has trouble with the App:

5.9.1. Should seek emergency assistance by calling their host country emergency number, UNDSS local emergency contact or the UNDSS 24/7 COMSCEN. All of which are provided in each location's Travel Advisory.

5.9.2. Should seek technical support via the link on the App.

5.10. If local eTA Command Center Administrators are unable to use the eTA for any of its functions, or if warranted by the Director, DRO, Deputy Director DRO or their designates, the UNDSS 24/7 Communications Center (COMSCEN) may be called to perform eTA Command Center functions, including activating GeoLocation and conducting an emergency headcount.

6. **How eTA works**

6.1. The eTA has two parts: the Desktop Command Center for security professionals and the App for all UN System personnel. Both are linked to several UNSMS datasets based in UNSMIN.

6.1.1. The information in the table below is provided by UNSMS datasets to the eTA App. This data will appear automatically on each App based on its location.

Data type	Data Source	Data location on App	Responsibility to provide and maintain
UN premises	UNSMS Premises Dataset	Homepage "Information" tab	UNDSS – country staff
Security Advisory ("Emergency Information")	Travel Advisory	Homepage "Information" tab	UNDSS – country staff
Security Clearance status	TRIP	Homepage "My profile" tab	Each UN System personnel
Emergency Contact	Travel Advisory	« Emergency » tab	UNDSS – country staff

6.1.2. The eTA Command Center provides a way for security professionals to interact with eTA App users in their AoR by sending notifications, conducting headcounts and providing the last known location of App users. The remainder of this SOP details procedures for each of these Command Center functions that involve real-time inputs from security professionals.

7. Procedures for Notifications

7.1. When warranted, the P/CSA/SA/CSO, on behalf of the DO, will send a DO-approved notification to all UNSMS staff in the impacted area immediately using the eTA Command Center as the primary means to communicate this security information to staff.

7.1.1. *The Security Notifications* feature of eTA allows Command Center Administrators 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 geo-fencing an area on the map interface of the eTA Command Center. These notifications are sent to all eTA end-users present in the pre-defined area or Operational Zone. The most senior security professional or designate should select the area to be notified based on operational needs.

7.1.2. There are three types of notifications:

7.1.2.1. *Security Alert*, when a security incident has occurred, (i.e. a suspicious package has been found);

7.1.2.2. *Security Warning*, when a security situation is imminent (i.e. demonstrations nearby, closing of streets, etc);

7.1.2.3. *Information Only*, when you want to inform of an event (i.e. training events, weather warnings, etc).

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

7.1.4. 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 language most appropriate for area and English.
4. In areas with unreliable connectivity, send secondary communication by established alternate means.

8. Procedures for Accounting for UNSMS Personnel

8.1. Emergency Headcount

8.1.1. In the event of an emergency/crisis, the most senior security professional of UNDSS in the Designated Area or designate will use the eTA Headcount feature as the primary means to account for UN System personnel who could be impacted by the 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.

8.1.2. After following the procedures for *Activating a Headcount Zone* detailed in the Headcount "How-to" manual, security professionals responsible for accounting for impacted UN System personnel will monitor the status of responses using the Headcount Status interface on the Command Center (shown) or by choosing the appropriate headcount report as filed in "I'm OK List by Date, Country and Agency," on UNSMIN.

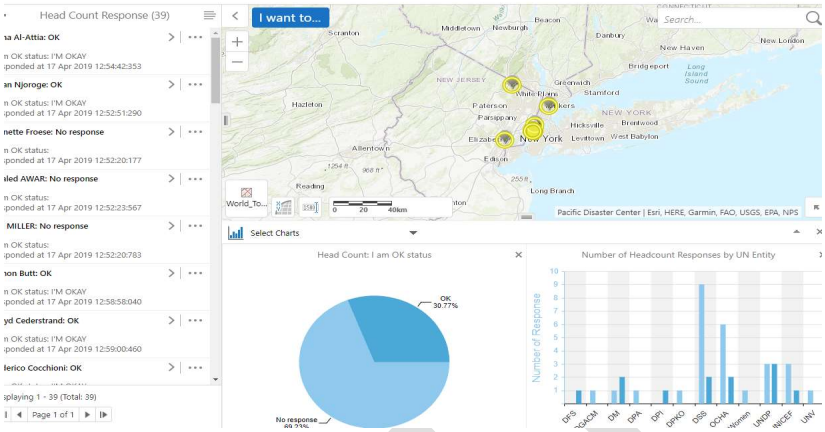

FIGURE 1 – ETA HEADCOUNT STATUS INTERFACE

8.1.3. Security personnel actions for each type of response received from UN System personnel via the eTA should include, but not be limited to the following.

8.1.3.1. In the case of a "NOT OKAY" response, local procedures for aiding staff should be followed. These can include, but are not limited to, activating the GeoLocation and/or Locate & Assist features on eTA to pinpoint or narrow down staff location. Every means necessary should be employed to locate staff and assist them.

8.1.3.2. In case of no response during the Head Count the existing procedure of finding/locating the staff should be followed and assistance provided as required.

8.1.3.3. To ensure all staff of each AFP that are impacted by an event are assisted, agency security professionals can use their own view of the headcount status to coordinate with UNDSS how best to assist AFP staff. It is the responsibility of the AFPs to follow-up with their own personnel.

8.1.4. The monitoring of the head count status will be pursued until directed to deactivate by the most senior security professional.

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

8.1.6. If local UNDSS staff are unable to conduct a headcount, this action can be undertaken by the UNDSS 24/7 COMSCEN as directed by the Director, DRO, or Deputy Director, DRO.

8.2. **Routine Headcount**
The eTA can be used for routine headcount procedures/warden system checks, as needed. 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 tool.

7.3 All headcounts are set to last no longer than 24 hours unless otherwise specified.

9. **Procedures for Activating the eTA GeoLocation feature**

9.1. ***The eTA GeoLocation feature can only be activated as approved by the DO or their designated alternate present in the AoR..***

9.2. Once activated, all users in the area where it is turned on *must be notified* of this action. A Quick Notification or Operational Zone Notification can be used to inform staff.

9.3. Upon activation of the eTA GeoLocation feature, the following information will be transmitted from the eTA App to the eTA Command Center where it will be visible to security personnel who are eTA Command Center Administrators for the Designated Area:

9.3.1. The last known location – as an icon on the map and as geocoordinates in the user data (see Figure 2) – of UN System personnel.

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

8.3.3 Security clearance status of each individual as represented by the colour of the icon associated with them.

FIGURE 2 – ETA USER LOCATION DISPLAY WITH GEOLOCATION ON

Blue represents personnel in their home duty station
Orange represents personnel travelling in the area WITH security clearance
Red represents personnel travelling in the area WITHOUT security clearance

9.3.4. Only eTA App users that have the location services for the App activated on their mobile device will be visible on the eTA Command Center. It is imperative that all eTA Command Center Administrators and other UNSMS security professionals instruct their personnel to download and *activate location and notification services* on the App.

9.4. The eTA GeoLocation feature should be turned OFF in every Designated Area, except in instances where it is a Security Risk Management Measure (SRMM) as approved by the DO and Security Management Team (SMT).

9.5. Activation of the GeoLocation feature is done by clicking on the "eTA Tools – SRM Area Setup" section of the eTA Command Center and selecting the appropriate SRM Area.

9.6. The eTA GeoLocation feature can be turned ON and can remain operational in a Designated Area as a SRMM approved by the DO/SMT in areas of high- or very-high-risk.

9.6.1. This action must be justified by an approved SRM and should stipulate a change in this functionality should changes in risk warrant.

9.6.2. UNSMS personnel must be informed of this activation as an SRMM.

9.6.3. DRO Desk must be informed of the activation.

9.7. The eTA GeoLocation feature can be turned ON for a limited time in the event of an emergency in a Designated Area as approved by the DO.

9.7.1. 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 staff.

9.7.2. This type of limited activation requires that the most senior security professional, consult with the DO, prior to activating the GeoLocation feature of the eTA application.

9.7.3. 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.

9.7.4. The eTA GeoLocation feature must be turned OFF when it is determined that all UN System personnel that could have been impacted by the event are accounted for and assisted, if required.

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.

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

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

10. **Procedures for the eTA Locate & Assist feature**

10.1. ***The eTA Locate & Assist (L&A) feature can only be activated as approved by the DO or their designated alternate present in the AoR..***

10.2. Once activated, all users in the area where it is turned on *must be notified* of this action. A Quick Notification or Operational Zone Notification can be used to inform staff.

10.3. The Locate & Assist (L&A) feature in the eTA allows for a lasting display of GeoLocations on the eTA Command Center, including paths between locations, for all eTA App users in a Designated Area. (Figure 3 – Visualization of L&A).

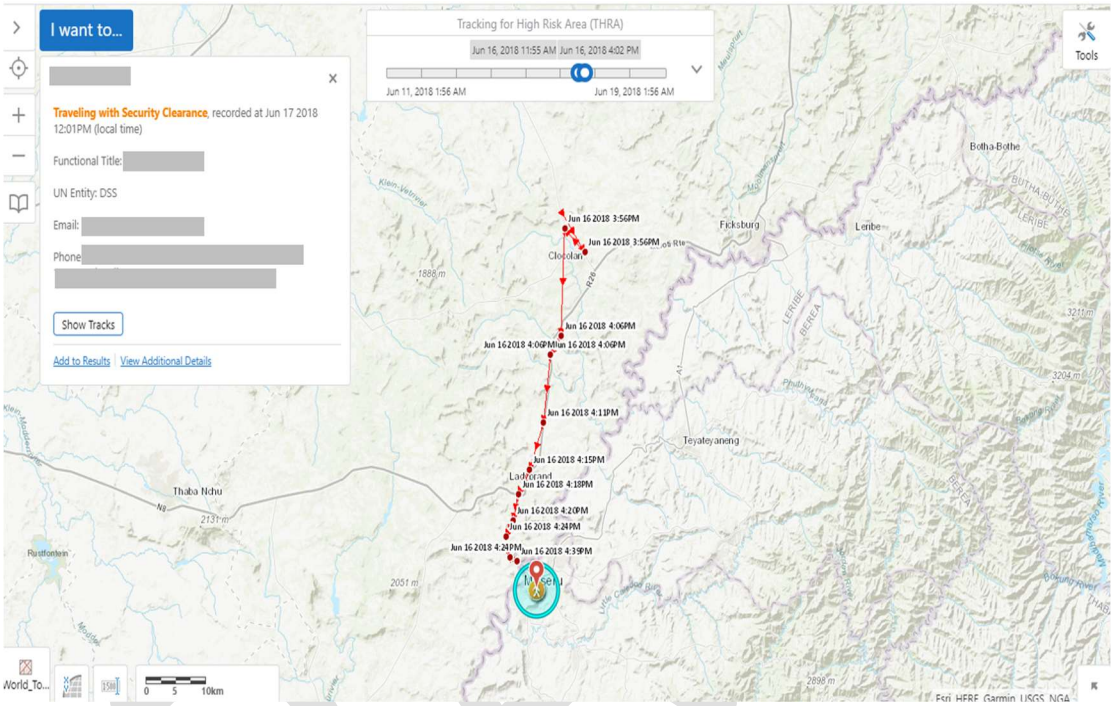

FIGURE 3 – VISUALIZATION OF ETA LOCATE & ASSIST FUNCTION

10.4. The eTA L&A feature can be turned ON and can remain operational in a Designated Area as a SRMM as approved by the DO/SMT in areas of high- or very-high-risk.

10.4.1. This action must be justified by an approved SRM and should stipulate a change in this functionality should changes in risk warrant.

10.4.2. UN System personnel must be informed of this activation as an SRMM.

10.4.3. DRO Desk must be informed of this activation as an SRMM.

10.5. Enabling the “Locate & Assist" function in an area is considered a measure to manage risk and should be the product of the SRM process. Users who do not comply with the requirement to use this functionality are subject to the same disciplinary measures available to the DO for UNSMS personnel who do not abide by SRM measures required for the location.

10.6. The most senior security professional remains responsible for the overall management and use of the eTA Application and will develop a local SOP to govern the process.

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

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

11. Procedures for Responding to Emergency

11.1. The "Emergency Contact" distress call button on the eTA App is an additional tool provided for UN System personnel who need assistance in times of emergency or similar situation.

11.2. The *Emergency Contact* button will be programmed to dial /connect to the most appropriate and effective responder in the geographic area.

11.2.1. The *Emergency Contact* button will automatically route the distress call to the host country authority if the host country is capable to respond appropriately to any kind of distress call with appropriate resources, and in a manner that will not cause further harm to the UNSMS personnel. In the event that UN personnel connect to host country authorities using the *Emergency Contact* button, no response from UNDSS is expected or required.

11.2.2. If host authority has limited/ no capacity to respond to any kind of distress call with appropriate resources and there is a UN 24/7 Security Operations Center with response capacity, the *Emergency Contact* button will route the distress call to the UN 24/7 Security Operations Center in the country where the distress call was made.

11.2.3. If host authority has limited/ no capacity to respond to any kind of distress call with appropriate resources and there is no UN 24/7 communications/radio room, calls from the *Emergency Contact* button should be routed to the UN Security Professional responsible for the area.

11.2.4. In the event that there is no host country capability and UNDSS local staff fail to respond within the designated timeframe, which should be within, but no longer than one hour, the 24/7 COMSCEN will promptly refer eTA emergency contacts to responsible UNDSS Desk Officers and Desk Chiefs and will monitor the response and follow-up.

9.2 UNDSS response to UN System personnel using the eTA *Emergency Contact* button should respond to and assist staff as defined by local SOP.

eTA Use in Contingencies

COMSCEN eTA = COMSCEN remote use of Command Center

IF these connections are lost… **…eTA can be used like this[5]**

Connectivity							Response						
DATA	VOICE	SMS	Landline	Radio	Sat phone		Concentration point	Hardcopylists (TRIP and staff)	COMSCEN eTA	Local eTA	Blackbox	Radio	Sat phone
Nil	Nil	Nil	Nil	Nil	Nil	→	Staff aware of conc pt	House-to-house and hotel accounting	**Used to get last known location. Results provided to first responders deployed and/or to HC**	N/A			
Nil	Nil	Nil	Nil	Nil	Yes	→	Same as above		**Used to get last known location. Results provided verbally via Sat phone**	N/A	Deployed to use with SAT technology		Used
Nil	Nil	Nil	Nil	Yes	Yes	→	Same as above		Same as above	N/A	Deployed to use with radio technology	Used	Used
Nil	Nil	Nil	Yes	Yes	Yes	→	Same as above	Lists used to call residences and hotels	**Same as above results faxed to local DSS**	N/A	Deployed to use with radio technology	Used	Used
Nil	Nil	Yes	Yes	Yes	Yes	→	Same as above	Lists used to send SMS and call staff	**Same as above results faxed and/or emailed to local DSS. eTA used to send notification as SMS. When available, eTA used to conduct headcount via SMS**	If WFP Black box deployed, can be used to send SMS messages	Deployed to use to send SMS		
Nil	Yes	Yes	Yes	Yes	Yes	→	Same as above	Lists used to send SMS and call staff	**Same as above results faxed/emailed/texted to local DSS. eTA used to send notification as SMS and to App. eTA used for headcount.**	Same as above	Deployed to use to send SMS and App		
Yes	Yes	Yes	Yes	Yes	Yes	→	Same as above	Lists used to send SMS and call staff		eTA used locally to get last known location of staff and staff status	N/A		

[5] The "Blackbox" is a WFP standalone tool that provides internet connectivity. It is not active nor has WFP provided any guarantees of providing it to support eTA. This is only conceptual.