European
Joint
Support Unit

Security

Izmir

European Joint Support Unit

Aim

The aim of this document is to define the process for contacting and establishing the GBR Contingent condition in response to an incident. It will define the tools for use and actions to be taken by both military and civilians serving within the community.

Assumptions

The following assumptions remain key drivers in the developed and maintenance of this process:

- The requirement to account for all serving members and their families is crucial within the SNR's Risk Management responsibility. It supports CO EJSU and wider MoD duty of care and is mandatory.
- The CDO must report back to LANDCOM/CoC within 2hrs of any activation on GBR accountability.
- The community must have declared their routine, primary and secondary contactable means with a copy held in the CDO Folder.
- Individual tracking will be supported by all ranks fulfilling the mandated 'out of station' administration for TDY, courses, leave or national business.
- Unless briefed on a change in the UK security posture, a community member could reasonably be away from Izmir during weekends or evenings without others in the community being aware.
- CAN 3.8 Technology Support has been read in conjunction and individuals have registered their routine, primary and secondary communication choices with the NSE.

Communication Platforms

To comply with privacy guidance (and maintain trust), access to personal contact details will be restricted. The CDO folder is to contain an extensive list of all known contact details which is SEALED and may only be opened if activation of this plan (or other emergency responses) is required. Those details will not be shared on public forums.

The following are used within the contingent for sharing a variety of information. They are trusted platforms that are ideally placed for exploitation as part of the emergency Focal Point architecture. The platforms to be exploited are listed below; those used during an emergency are highlighted in RED:

European
Joint
Support Unit

Platform	% Coverage of GBR Members	Remarks
Turkish/UK Mobile Phone	All	May not have data access for WhatsApp, but could still make calls (subject to connection)
WhatsApp Check In Group	Very High %	Service persons and staffs, limitations if mobile
WhatsApp Gurel Group	100%	All living in the Gurel tower, limitations if mobile
WhatsApp Wives Group	?	Coverage is not known, limitations if mobile
Facebook TRIB Turkey	High %	Has limitations for some data users if mobile
Facebook Private Messenger	High %	Has limitations for some data users if mobile
Email	High %	Has limitations for some data users if mobile

European Joint Support Unit

Activation Procedure

Driver or Mechanism	Requirement	Response
LANDCOM OPSCEN **SNR** **EJSU** **Natural Disaster** **Obvious risk to contingent**	Accountability of a specific person or all personnel in the contingent within 2hrs.	Activate the Security and Focal Point Plan
Sent out via: **1. WhatsApp Check In Group** **2. Text** **3. Facebook** **The Contact List Preferences held in the CDO Folder is to be used to identify individual contactable means.**	**CHECK IN ACTIVE** + 'Brief explanation of the threat'	All contingent must respond within 2hrs with a mobile text to the CDO or WhatsApp Check In Group message stating information about: 1. Name ((s) if in a group) and location. 2. Names and locations of those family members not in that group - but of a known whereabouts. 3. Names and possible locations (if known) of those family members not unaccounted for. CDO updates the nominal roll of those accounted for.
ALL COMMUNITY MEMBERS ARE TO CEASE USE OF THE PORTALS AND MINIMISE DESTRACTING INFORMATION TO ENABLE THE FACTUAL HEAD COUNT TO BE COMPLETED WITHIN 2 HRS		
CDO investigates non responders to the initial ACTIVE message	NSE staffs may be required to interrogate JPA for leave, TDY or course locations.	CDO uses direct communications with those yet to respond or who may not be in country to ascertain if they are OK.
90 minutes after the initial activation a second message is sent	**CHECK IN CLOSES IN 30 MINUTES** + Relevant update	Those respondents to the first message do nothing. CDO continues to establish communications with those still not found using personnel secondary contact means.
2hrs after initial ACTIVE message a final message is sent.	**CHECK IN CLOSED** + Brief explanation of what threat remains and action to take	CDO reports the final status/location of known community members and a list with potential locations of those not contactable to the following: 1. SNR 2. LANDCOM OPSCEN 3. Contingent Commander
Feedback and continued support	The CDO provides a releasable situational update via WhatsApp and Facebook.	No response is required from staffs
ALL PORTALS ARE OPEN FOR NORMAL BUSINESS		

European
Joint
Support Unit

ALL COMMUNITY MEMBERS ARE TO CEASE USE OF THE PORTALS AND MINIMISE DESTRACTING INFORMATION TO ENABLE THE FACTUAL HEAD COUNT TO BE COMPLETED WITHIN 2 HRS		
CDO investigates non responders to the initial ACTIVE message	NSE staffs may be required to interrogate JPA for leave, TDY or course locations.	CDO uses direct communications with those yet to respond or who may not be in country to ascertain if they are OK.
90 minutes after the initial activation a second message is sent	**CHECK IN CLOSES IN 30 MINUTES** + Relevant update	Those respondents to the first message do nothing. CDO continues to establish communications with those still not found using personnel secondary contact means.
2hrs after initial ACTIVE message a final message is sent.	**CHECK IN CLOSED** + Brief explanation of what threat remains and action to take	CDO reports the final status/location of known community members and a list with potential locations of those not contactable to the following: 1. SNR 2. LANDCOM OPSCEN 3. Contingent Commander
Feedback and continued support	The CDO provides a releasable situational update via WhatsApp and Facebook.	No response is required from staffs
ALL PORTALS ARE OPEN FOR NORMAL BUSINESS		

European
Joint
Support Unit

Home Security

If you have an alarm, make sure it is set, working properly and don't leave sensors covered. Make sure all doors and windows are locked.

If you have a door lock or window locks make sure they are serviceable, and you use them.

If you have an internal door between your SFA and garage, consider this as an external door and ensure it is secured appropriately.

Don't leave door keys within sight or reach from anyone outside. Potential thieves have been known to 'fish' keys through letterboxes or windows that have been left open. This also applies to car keys.

Open/Close shutters.

Purchase a Wi-Fi security camera for your home (i.e. Ring). These are very reasonable and can be purchased from the internet and will allow you to view your home when you are away. You will have seen adverts on the TV for wireless cameras for your front door, there are some good alternatives for sale on Amazon which are relatively inexpensive and easy to install.

Use time clocks to show lights in your home during the evening and early morning. Try to use the time clocks with a feature of several days and do not set everyday with the same time, a radio on a timer is also a great deterrent. This will give the impression of a normal pattern of life and deter any would be burglar.

Don't advertise your planned period away on Social Media, people use Social Media to check for holidays to select houses to break in to.

Park your vehicle near the garage door so it cannot be opened.

If leaving your property vacant, contact the local police and see if they offer a 'Homewatch' scheme. They will arrange for extra police patrols to cover your street and will pay attention to your home address. The form is available on-line, from the police or BSG. If they don't offer this service, ask a friend/neighbour to check on your property and pick up the post.

European
Joint
Support Unit

Cold Callers

Receiving unwanted callers on your door step when living in a foreign country can be very daunting. All official callers should notify DIO first, who will then book an appointment with you. Workmen should not turn up unexpectedly, if they do turn them away.

Here is some guidance to help deal with these callers

- Put a sign on your door, ask your CLO for some advice.
- If someone knocks the door:
  - Do not open the door fully. If you have a safety chain use it.
  - Check ID
  - Confirm what they are here for, are they asking a lot of questions?
  - Politely turn them away
  - Contact DIO/NSE and detail what has happened
- Get a social media group together, where you can forewarn each other that people are in the neighbourhood.

Use of Social Media

Most people think a Virtual Private Network (VPN) is just another way to watch UK TV in Europe.

It is also the best way to secure your internet, protect your personal information and the information you are sending/receiving when using the internet.

WIFI hotspots that don't ask for a log on or password to use are particularly vulnerable to hackers who will intercept your information. This could lead to your identity being stolen or your bank details being copied.

It is recommended that you use a VPN to secure yourselves. Some are free and some you purchase. A paid for VPN provider is more secure than a free VPN, as free VPN providers tend to sell your information on to make a profit. Some VPN providers to consider are:

- NordVPN
- PureVPN
- ExpressVPN

European
Joint
Support Unit

Internet Searches

The term ‘let’s Google it’ is common place nowadays. But have you noticed that Google seems to already know where you want to look, and it knows what you have recently purchased? That’s because they store your search information. If you want to remain anonymous, use these search providers:

- Mozilla Firefox
- DuckDuckGo

Fitness Apps and Tracking Devices

Most of us use fitness tracking devices, be it via smart phone or through a smart watch. There is evidence to suggest that these devices are tracking our movements and sharing our data.

If you use these devices it is suggested that you follow these easy steps:

- Lock down/apply privacy settings on any media account where location data could be available to prevent unauthorised/uninvited access.
- Opt out of any heat map data collection or enable privacy zone functionality using application settings
- Turn off GPS on any application when not required.

Phishing Scams

Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person, through email and other communication channels, to induce individuals to reveal personal information such as passwords and bank account details.

Phishing scams have been around since the internet first existed and are not likely to disappear any time soon. There are however several ways you can prevent falling victim such as using Antivirus Software and Firewalls and thinking before you click.

For further information on cyber security advice to protect you and your family visit www.ncsc.gov.uk/section/information-for/individuals-families

European
Joint
Support Unit

Country Advice

Certain countries hold a very real threat to military personnel, be that from espionage or terrorism. Before travelling to a country, you believe may be of interest, first check the FCO website –

https://www.gov.uk/foreign-travel-advice

If you haven't already, download the Travel Oracle App. Details available from the CLO.

CSSRA/High Threat Countries – those with DV

If you are travelling to Countries to which Special Security Regulations Apply (CSSRA) or High Threat Countries, whilst not prohibited, it is essential that you contact EJSU J2, who will be able to offer you guidance on these locations. The CSSRA list and associated guidance can be found in DI-CI Overseas Travel Guide (for MODNET only).

If you have any further travel queries, please contact EJSU J2 who will be able to offer more guidance. EJSU-J2-Mailbox@mod.gov.uk