ARMY CRIMINAL INVESTIGATION DIVISION

4 February 2025

Cybercrime Prevention Flyer

U.S. - Mexico Border Operations: Cell Tower OPSEC

Soldiers and government personnel assigned to U.S. and Mexico border operations face the risk of their government and non-government mobile devices connecting to cell towers and/or networks across the international border. This risk inherently increases the vulnerability to personnel, and their mobile devices from malicious, criminal and foreign government actors attempting to gain unauthorized access to devices, conduct surveillance, or undertake influence operations.

While U.S. telecommunication companies do maintain and operate cell towers in Mexico, it is possible a mobile device used in the U.S. could connect with a Mexican telecommunication company's tower or the tower of a nefarious actor operating an international mobile subscriber identity (IMSI) catcher mimicking a legitimate cell tower. Whether a legitimate Mexican telecommunication tower or a rogue tower operating as a man-in-the-middle, a hostile actor could intercept and capture data, calls, and texts, conduct surveillance by tracking location information, collect a device's IMSI number, collect phone numbers, monitor calls, distribute malware to a device, and/or potentially steal sensitive information.

To mitigate such risks, soldiers and government personnel assigned to border operations should:

- Use a virtual private network (VPN) to encrypt internet traffic and mask the IP address used by the mobile device, making it more difficult to intercept communication or track location.
- Consider using secure messaging applications to encrypt communication to protect conversations.
- Limit transmitting sensitive, confidential, financial, or personal communication via unencrypted methods.
- Avoid using public Wi-Fi networks as they are often less secure and expose communication to interception.
- Avoid answering calls and responding to texts from unknown phone numbers.
- Disable device data roaming and international roaming. Cell phones and other mobile devices do not recognize international borders and will select the tower providing the best signal, even if it is not the nearest tower.
- Disable device location services. If device location settings must be turned on, review the settings of each individual application and adjust the application permissions to the appropriate level.

Additional OPSEC measures include:

- Review social media applications to ensure location tracking and tagging is turned off.
- Be cautious when posting a picture even when location tagging is turned off. Pictures are often revealing, providing potential intelligence.
- Disable public sharing of social media information.
- Do not click on suspicious links.

Authorized for widest release, without restrictions.

To receive Cyber Field Office Cybercrime Prevention Flyers, send an email to: CYDIntel@army.mil

CPF 0011-2025-CID461

Cyber Field Office
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134

SUBMIT A TIP
REPORT A CRIME
WWW.CID.ARMY.MIL

CID LOOKOUT
ON POINT FOR THE ARMY