## Civil Defence Communications

Draft 1 – version 1:

There are commercially available solutions that can help facilitate secure communications using encryption methods suitable for post-EMP scenarios, including but not limited to the concepts similar to the one-time pad (OTP). Here are some options:

**Commercially Available Communication Equipment**

1. **Digital Ham Radios**
   - **Examples**: Icom IC-7300, Yaesu FT-991A
   - **Features**: These devices support various digital modes (like PSK31, FT8) that can be used to transmit encrypted text messages.
   - **Usage**: Suitable for communicating encrypted messages over long distances using HF bands.
2. **Civilian Encryption Devices**
   - **Secure Voice and Text**: Commercial devices that offer secure voice and text communication using strong encryption.
   - **Examples**: Secure phones or radios from companies like Barrett Communications (e.g., PRC-2090 HF Radio), which can include built-in encryption features.
   - **Usage**: More suitable for organizations that require robust, secure communication methods.
3. **Encryption Software**
   - **Examples**: Software like VernamCipher (an implementation of OTP) can be used to encrypt and decrypt messages on a computer before sending them via radio.
   - **Usage**: Encrypt messages on a laptop or mobile device before transmission. The ciphered text can be transmitted via any digital mode over the radio.
4. **Portable Satellite Communication Devices**
   - **Examples**: Garmin InReach, Iridium GO!
   - **Features**: These devices provide satellite-based communication capabilities, which could be an alternative if traditional radio frequencies are compromised.
   - **Usage**: For encrypted text, you must use an external software application to secure the message before transmission.
5. **Faraday Cages and Bags**
   - **Examples**: Mission Darkness, Faraday Defense products
   - **Usage**: To protect electronic devices from EMP effects, store critical communication devices and encryption tools in Faraday cages or bags.

**Special Considerations for Using OTP and Encrypted Communication**

1. **Pre-distribute Keys**: For OTP usage, pre-distribute physical key books to trusted parties with strict handling protocols.
2. **Training**: Ensure all users are trained in both the operation of radios and in the encryption/decryption process to avoid errors.

3. **Backups**: Keep multiple copies of key materials in different locations to ensure availability even if an EMP disrupts the primary site.
4. **Practice Drills**: Conduct regular