# Civil Air Patrol




## COMSEC & OPSEC

## Briefing for Communications Managers

Ed Wolff

7 August 2019

ONE CIVIL AIR PATROL, EXCELLING IN SERVICE TO OUR NATION AND OUR MEMBERS!

# Consider some of the following "traditional" security programs:

- *Personnel Security*
  - *Personally Identifiable Information*
    - *Names, telephone numbers, addresses, call signs*
- *Physical Security*
  - *Security of repeater sites*
  - *Security of radio equipment*
- *Communications Security*
  - *Using encryption on VHF*
  - *Using off line encryption*
- *Information Security*
  - *Encrypting files posted to the internet*
  - *Using password protected, member access web sites as compared to public facing sites*

# OPSEC Program

- 18 August 2017 CAP OPSEC Officer and Asst OPSEC Officer Appointed
  - LtCol Ed Wolff, HQ OPSEC Officer
  - LtCol Brian Falvey, HQ Asst OPSEC Officer
- Approved to establish joint CAP-USAF OPSEC Working Group with HQ CAP-USAF
- Initial Critical Information List (CIL) developed
- CAP-USAF staff assignment to OPSEC WG pending

# Do we need a security program?

- XX Wing- PDF file that provides calls signs
- X Region Communications Guidebook providing calls signs
- XX Wing- Communications Exercise Plan with names, phone numbers, call signs, etc.
- XX Region- Exercise Plan
- XX Wing- Call sign list document
- XX Wing- Call sign list
- XX Wing- Call signs on web page
- XX Region- Cal sign list

# When can OPSEC be used?

- Communications Training Exercises
- Communications Plans and Standard Operating Procedures
- Communications Methods, Sources, and Technical Tradecraft (Code Plugs)
- Software and Source Code, P/W protect code plugs
- PIO/PAO releases
- Personal social media published information

# Every Person Is An OPSEC Sensor!

Every person in your squadron, group, wing, region is a part of the security solution by:

- ✓ Knowing the threats
- ✓ Knowing what to protect
- ✓ Knowing how to protect it!



# Critical Information List

CAP C.I.L. for OPSEC Survey

- Personally Identifiable Information (PII)
- Call signs
- Frequencies and Radio Code Plugs
- Net schedules
- Mission specific details
  - CD missions, Green Flag, HLS Missions, AD Missions
- Operations and Exercise Plans
- Infrastructure Information- repeater locations

# A note on public websites:

Certain things should not be found on public websites, blogs, etc., including:

- Sensitive Operations Plans
- Sensitive Communications Plans
- Alerting Lists, With Names
- By Name Personnel Lists
- Locations of Sensitive Assets (Vehicles, Airplanes, Radios, etc.)
- Locations of Sensitive Facilities (EOC's, COOP Sites, etc.)

"The internet"

# Open Source Intelligence

AKA- One of the greatest threats to any organization

1. Publically available information that any member of the public may lawfully obtain my request or observation.
2. Unclassified information that has limited public information or access
3. 80-85% of intelligence can be gathered using OSINT



Source: re-configure.org

# “It” never goes away!

When you put information on the net, via your blog, Facebook, email, etc., you have to assume that it’s going to stay there forever.

Same thing with newspapers, magazines, and other media.

The only safe bet is to make sure that it never gets there in the first place!

# COMSEC

- What is COMSEC?
- What is a Controlled Cryptographic Item (CCI)?
- Examples of CCI
- Access
- Safeguarding
- Reporting Requirements
- Contacts

# What is COMSEC?

COMSEC (Communications Security) –

Broad term used to describe the measures and controls taken to deny unauthorized persons information derived from various communication sources and ensure the authenticity of such communications.

# What is COMSEC?

- These items can be further categorized into:
  - Cryptographic key material (CRYPTO)
  - Controlled Cryptographic Items (CCI)
  - Classified devices
    - ✓For purposes of this briefing, we're concerned with Unclassified CCI only

# Communications Security

- P25 digital mode adds a level of security to the network.
- USAF funded the P25 transition almost 20 years ago and supplied radios per the NHQ TA
- Type 3 AES encryption provides a higher level of security for voice communications on missions, especially CD and discrete AF missions.
- New TA includes KVLs for deployment to the field
- Currently using the NLECC KMF for key management
- NHQ/DOKS is the single POC with the NLECC

# Communications Security

- CAP has four keys assigned at the NLECC
- 2019 encryption keys- 4 static AES keys
- Interop keys are loaded on a case by case basis with approval of NHQ/DOKS
- All radios will have place holders in the code plug for all 20 interop keys
- Keys for other agencies will only be loaded with the approval of NHQ/DOKS, this is a liability issue.
- If a radio is lost, stolen, or a member refuses to return a radio that is key loaded it may cause the entire country (all radios across all federal-state-local agencies to require re-keying!

# Communications Security

- KVL security
  - KVL5000w ordered
  - A KVL is considered a controlled item and will be issued based upon a hand receipt
  - A KVL must be secured in a locked cabinet when not in use and is the responsibility of the assigned custodian
  - A KVL is not to be packed in checked luggage, left in an unattended vehicle, left in an unattended office, etc.



# Enforcement

- CAP does NOT have a COMSEC account.
- CAP is only a user of unclassified but controlled equipment supplied by another agency.
- This is not your typical CAP equipment accountability.
- CAP and its members are legally liable for the improper access, storage, or use of CCI equipment.
- Title 18, United States Code, sections 641, 793, 798, and 952.

# Physical Security of CCI

- COMSEC Material Control System is used to distribute accountable COMSEC items to include unclassified CCI equipment, maintenance manuals, and keying equipment.
  - Some military departments have been authorized to distribute CCI equipment through their standard logistics system.
  - The recipient (CAP) must get a hand receipt for acceptance of the equipment and complete any supplying agency required training and briefings.

# Devices

## CONTROLLED CRYPTOGRAPHIC ITEM

- Unclassified cryptographic device
- Protected as high value property
- Accountable to the National Security Agency
- Identified by nomenclature: NSA issued short title
- Examples of short titles:
  - PRC117G
  - AN ARC 231 V C
  - KSV 21

CCI can always be identified by the “Controlled Cryptographic Item CCI” marking on the item’s faceplate

# KSV 21 card for STE

- Secure Telephone Equipment (STE)
- Secure point-to point voice/data communications up to Top Secret
- Unclassified with out the KSV 21 card
- Only the KSV 21 card is accountable



# PRC 117G




Controlled Cryptographic Item (CCI)
Unclassified without classified key material loaded

# Access Requirements

- Pursuant to Title 18 USC the following minimum conditions must be met prior to granting access to Unclassified CCI:
  - Need-to-Know determination
  - United States Citizenship
  - Receive Unclassified CCI Access Briefing from the agency providing the CCI equipment and have completed this generic CAP CCI over-view briefing.

# Safeguarding

Unclassified CCI

- If not being used or attended by a briefed individual, must be secured behind a locked door, storage room, etc. and sighted regularly

- If installed in an aircraft, authorization to leave unattended depends on the physical security controls in place to prevent removal of the installed equipment from the aircraft. As a rule it will not be left unattended but if it must be then security must be in place. Only persons with direct access need to be briefed.

# Safeguarding

Do NOT:

- Provide supplied CCI equipment to anyone without verifying completion of a CCI access briefing
- Move CCI to another location (permanent location) without coordinating hand receipt movement with the Communications Security Division or designee.

- Cadet members may not be left in sole possession or control of any CCI equipment.

# Safeguarding

Hand Receipt Items

- Items Hand Receipted to you by the entity providing the CCI equipment becomes your personal responsibility and may never be transferred by you to another person or organization without authorization.

- To formally transfer CCI, you must contact the originally issuing entity that “owns” the CCI equipment.

- Another properly briefed person (not a cadet) may use your items but this does not relieve you of its responsibility

# Reporting Requirements

- Report any suspected tampering or misuse of CCI to the COMSEC Custodian immediately
- Why is it so important to protect CCI?
  - The War Fighter will eventually communicate classified information with these devices
  - Attempts to reverse engineer the CCI
  - Ultimately accountable to the National Security Agency

# Conclusion



OPSEC is what you make of it.

- The way ahead
  - Annual OPSEC training requirements in compliance with AFI 10-701
  - OPSEC Survey
  - OPSEC evaluations of CAP web sites (already started from the DOK side)
  - OPSEC awareness emphasis at the Squadron, Group, Wing, Region and National levels.
  - New emerging missions will drive this requirements for enhanced OPSEC awareness

# Questions


**LtCol Ed Wolff, AFAUX/CAP**
**NHQ OPSEC Officer**
**NHQ Division Head**
**Communications Security**

**ewolff@capnhq.gov**
**Edward.wolff.1@us.af.mil**
**Edward.wolff@us.af.smil.mil**


CELEBRATING
Our Partnerships