COM-03 COMSEC — Communications Security

Protecting what your traffic says, not just whether it gets through.

BOTTOM LINE UP FRONT

COMSEC is the practice of protecting the content of your communications from being read or understood by someone who intercepts them. It is distinct from EMCON (protecting whether you're transmitting at all) and from net discipline (making sure a message gets through correctly). COMSEC covers code words, authentication, encryption, and disciplined handling of key material.

WHY THIS MATTERS

Anyone with a scanner can hear your net. COMSEC decides whether hearing it tells them anything.

Radio traffic in the clear is radio traffic anyone can monitor, including people you don't want listening. COMSEC gives a MAG the tools to keep operational content protected even when the transmission itself is not: code words for sensitive locations and people, authentication so members can verify who they're really talking to, and disciplined handling of any key material used for actual encryption.

► **COMSEC without key discipline is theater. A code word used the same way every time is not a code word — it's a pattern.**

THE FOUR COMSEC DISCIPLINES

Physical Security	Protecting COMSEC material — pads, code lists, authentication tables — from capture, theft, or observation.
Transmission Security	Reducing what an interceptor learns from traffic analysis even without breaking the content: call sign discipline, transmission length, timing patterns.
Cryptographic Security	The strength and correct application of whatever code or cipher is used, including proper one-time pad discipline.
Emission Security	Preventing the signal itself — a repeatable transmitter fingerprint, for example — from revealing information on its own.

COURSE LESSONS

1	**What COMSEC Protects (and What It Doesn't)** Distinguishes COMSEC (content) from EMCON (signature) and net discipline (accuracy). Opening scenario: a location code word used the same way every day.
2	**The Four COMSEC Disciplines** Physical, transmission, cryptographic, and emission security, defined with civilian MAG examples for each.
3	**Code Words & Authentication** Building a group code word list, challenge/reply basics (full treatment in COM-06), and rotation and compromise procedures.
4	**Key Material Discipline** Safe generation, storage, use, and destruction of any cryptographic key material. Connects to COM-07 One Time Pads for the full OTP procedure.
5	**Recognizing and Responding to Compromise** Indicators that a code word, key, or procedure has been compromised, and the group's response: what to change, how fast, and how to notify all stations.

DOCTRINAL SOURCES

CNSSI 4009	**National Information Assurance Glossary**	Defines the four COMSEC disciplines used as this course's core framework
ACP-122	**Communications Security (General)**	Allied doctrine on physical and cryptographic handling of communications security material
FFTP COM-07	**One Time Pads**	Companion course for the cryptographic security discipline covered here at overview level