



ELYRION COMSEC DIVISION

COMSEC ASSURANCE PROTOCOLS

PROTECTING WHAT MATTERS. ENABLING THE MISSION.



OUR MISSION:

To ensure the confidentiality, integrity, and availability of mission-critical communications through disciplined management of COMSEC systems, key material, and cryptographic assets in accordance with DoD and NSA policy.



PROTECT
People, Information,
and Networks



PRESERVE
Cryptographic
Assurance



ENABLE
Secure Global
Communications



DELIVER
Mission Readiness
and Confidence

1 CORE DoD POLICY — DoDI 8523.01



DoD Instruction 8523.01 establishes policy, assigns responsibilities, and provides procedures for managing COMSEC across the Department of Defense.



APPLIES TO: All DoD components and activities involved in acquisition, operation, and maintenance of COMSEC products and services.



KEY RESPONSIBILITIES:

- DoD CIO – Overall policy and oversight
- DIRNSA/CHCSS – COMSEC program management, key control, and security oversight
- DoD Component Heads – Implement COMSEC policy within their organizations



PROCEDURES COVER: COMSEC product acquisition, requirements, planning, and operational controls.

2 CONTRACTOR & INDUSTRIAL COMSEC — 32 CFR 117.21



Under the National Industrial Security Program Operating Manual (NISPOM), contractors must establish and maintain robust COMSEC programs when working with the U.S. Government.



APPLIES TO: Contractors using, installing, maintaining, or developing COMSEC systems for the U.S. Government.



ACCOUNT ESTABLISHMENT: Requires a COMSEC account with appropriate clearance (final PCL) for the FSO, COMSEC Account Manager, and alternate.



ACCESS RULES:

- TOP SECRET cryptographic material requires final TOP SECRET clearance.
- Interim TOP SECRET clearance is valid for SECRET/CONFIDENTIAL levels.



PROCEDURES: Contractors must follow COMSEC material control and operating procedures provided by the agency COR. These procedures may exceed baseline requirements.

3 NAVY-SPECIFIC PROTOCOL — SECNAVINST 2200.6



The Department of the Navy implements COMSEC policy in alignment with DoD directives and NSA authorities to ensure operational compliance and mission assurance.



APPLIES TO: All Navy and Marine Corps installations, commands, and systems (including contractor-operated).



POLICY: Establishes COMSEC monitoring, reporting, and compliance requirements; ensures alignment with DIRNSA/CHCSS and NSA/CHCSS authorities.



SCOPE: Covers all DON-owned/controlled telecom and information systems. Excludes intelligence-specific monitoring conducted under other authorities.

KEY MANAGEMENT PRINCIPLES



CLEARANCE & ELIGIBILITY

Only personnel with the appropriate final PCL may access or handle COMSEC material.



ACCOUNT CONTROL

COMSEC accounts require formal establishment, documented procedures, and oversight.



KEY SAFEGUARDING

All key material is controlled, inventoried, and protected per DoD and CNSS standards.



OPERATIONAL SECURITY

COMSEC systems must be operated in compliance with technical and administrative security measures.



AUDIT & COMPLIANCE

Programs are subject to inspection, accountability, and continuous compliance with policy.



COMPLIANCE. ACCOUNTABILITY. ASSURANCE.

Ensuring secure communications today to protect tomorrow's mission.



POLICY



NSA / DIRNSA



DON / SECNAV

OUR COMMITMENT

Elyrion COMSEC Division is committed to executing and exceeding all COMSEC requirements with precision, discipline, and integrity. We protect cryptographic assets so our customers can focus on their mission.

