



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, DC 20350-2000

OPNAVINST 5450.345  
DNS-33  
04 April 12

OPNAV INSTRUCTION 5450.345

From: Chief of Naval Operations

Subj: MISSION, FUNCTIONS, AND TASKS OF COMMANDER, U.S. FLEET  
CYBER COMMAND AND COMMANDER, U.S. TENTH FLEET

Ref: (a) OPNAVNOTE 5400 Ser DNS-33/12U102020 of 1 Mar 12  
(Canc frp: Mar 13)  
(b) DoD Instruction O-3115.07 of 19 Nov 10  
(c) DoD Directive 5100.20 of 26 Jan 10  
(d) OPNAVINST 3430.25  
(e) U.S. Navy Regulations 1990  
(f) OPNAVINST 5239.1C

Encl: (1) Functions and Tasks of COMFLTCYBERCOM and COMTENTHFLT

1. Purpose. To publish the authorities delegated to Commander, U.S. Fleet Cyber Command (COMFLTCYBERCOM) and Commander, U.S. TENTH Fleet (COMTENTHFLT) and the functions and tasks of U.S. Fleet Cyber Command (FLTCYBERCOM) and U.S. TENTH Fleet (TENTHFLT).

2. Background

a. The Chief of Naval Operations (CNO) established FLTCYBERCOM on 29 January 2010 as an echelon 2 command to serve as the Navy Component Command (NCC) to United States Strategic Command (USSTRATCOM) and United States Cyber Command (USCYBERCOM), providing operational employment of the Navy's cyber, network operations (NETOPS), Information Operations (IO), cryptologic and space forces, and to serve as the Navy's Service Cryptologic Component (SCC) commander to the National Security Agency/Central Security Service. TENTHFLT was re-commissioned to control operations supporting FLTCYBERCOM.

3. Authorities (as further detailed in enclosure (1))

a. COMFLTCYBERCOM, as directed by the Secretary of Defense, is assigned to serve as the NCC to USSTRATCOM for space operations, cyberspace operations and IO. COMFLTCYBERCOM is assigned by USSTRATCOM to serve as the Navy cyber component

commander to USCYBERCOM for cyberspace operations. COMFLTCYBERCOM is delegated operational control (OPCON) over Navy space and cyber forces assigned to USSTRATCOM.

b. COMFLTCYBERCOM is designated and assigned by the Secretary of the Navy to serve as Commander, Navy SCC to the Director, National Security Agency (DIRNSA)/Chief, Central Security Service (CHCSS). Per references (b) and (c), the SCC serves as the primary Service authority for all operations, programming, budgeting, training, personnel, policy, doctrine, and foreign relationships for cryptologic activities.

c. CNO designates COMFLTCYBERCOM to serve as the "central operational authority" for Navy networks, cryptology, SIGINT, IO, cyber, EW and space. Navy networks include all networks operated or defended by the Navy to include enterprise, legacy, and excepted networks with the exception of network elements that perform combat and weapon system, fire control, flight, and hull, mechanical and electrical control functions. FLTCYBERCOM exercises its operational authority to safeguard the interface between Navy networks and those network elements that perform combat and weapon system, fire control, flight, and hull, mechanical and electrical control functions.

d. COMFLTCYBERCOM's authorities regarding requirements, budget, and capabilities development are delineated in paragraph (8) of enclosure (1).

e. Per reference (d), COMFLTCYBERCOM, as the successor to Naval Security Group Command, is the executive agent for IO and EW within the Navy.

f. COMFLTCYBERCOM is appointed the operational designated approval authority (ODAA)/Authorizing Official (AO) for collateral and general services, classified and unclassified, information systems, networks, and telecommunications systems.

g. COMFLTCYBERCOM is the Navy's cyber claimant, budget submitting office (BSO) 60C.

#### 4. Missions

a. COMFLTCYBERCOM has the following missions:

(1) Serve as the central operational authority for networks, cryptologic and SIGINT, IO, cyber, EW and space capabilities in support of forces afloat and ashore.

(2) Direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace.

(3) Organize and direct Navy cryptologic operations worldwide and support IO and space planning and operations, as directed.

(4) Execute cyber missions, as directed.

(5) Direct, operate, maintain, secure and defend the Navy's portion of the Global Information Grid (GIG).

(6) Deliver integrated cyber, IO, cryptologic and space capabilities.

(7) Deliver global Navy cyber common operational picture.

(8) Develop, coordinate, assess and prioritize Navy cyber, cryptologic and SIGINT, space, IO and EW requirements.

(9) Assess Navy cyber readiness.

(10) Manage man, train and equip (MTE) functions associated with NCC and SCC commander responsibilities.

(11) Exercise ADCON and OPCON of assigned forces.

b. COMTENTHFLT has the following missions:

(1) Serve as the numbered fleet commander for COMFLTCYBERCOM and exercise OPCON of assigned naval forces.

(2) Coordinate with other naval, coalition and joint task forces to execute the full spectrum of cyber, EW, IO, and SIGINT capabilities, and missions.

## 5. Command Relationships

a. COMFLTCYBERCOM and COMTENTHFLT. COMFLTCYBERCOM and COMTENTHFLT are shore-based fleet activities in an active and fully operational status under the same commander. The commands operate as a single integrated headquarters, sharing operational and administrative support resources, but preserve the theater level and operational level and echelon 2 or echelon 3 level relationships. COMFLTCYBERCOM reports to the CNO for administrative and service related matters.

b. Administrative Chain of Command

<u>Echelon</u>	<u>Command</u>
1	Chief of Naval Operations
2	Commander, U.S. Fleet Cyber Command
3	Commander, U.S. 10th Fleet

c. Area Coordination Responsibility

(1) Commander, Navy Installations Command exercises area coordination responsibilities.

(2) Commander, Naval District Washington exercises regional coordination responsibilities.

d. Immediate Superior In Command (ISIC). COMFLTCYBERCOM is the ISIC for the following echelon 3 commands and has ADCON of the following assigned echelon 3 commands and their subordinate commands and detachments, per reference (a):

(1) Navy Information Operations Command (NIOC) Bahrain, Colorado, Georgia, Hawaii, Maryland, Menwith Hill, Misawa, Norfolk, Pensacola, Sugar Grove, Texas, and Yokosuka.

(2) Navy Cyber Warfare Development Group (NAVCYBERWARDEVGRU).

(3) Naval Computer and Telecommunications Area Master Stations (NCTAMS) Atlantic and Pacific.

(4) U.S. Naval Computer and Telecommunications Stations (NCTS) Bahrain, Naples, Sicily, and Far East.

(5) Naval Satellite Operations Center (NAVSOC).

(6) Navy Cyber Defense Operations Command (NCDOC).

(7) Naval Network Warfare Command (NAVNETWARCOM).

e. MTE. COMFLTCYBERCOM, as the designated commander of the Navy's SCC, is responsible for MTE functions of the Consolidated Cryptologic Program (CCP) funded cryptologic workforce in accordance with reference(c). Commander, U.S. Fleet Forces Command (COMUSFLTFORCOM), through NAVCYBERFOR, the global command, control, communications, computers, combat systems and intelligence (C5I) type commander, is responsible for MTE activities that support readiness of all cyber forces afloat and ashore (other than the CCP funded cryptologic workforce). COMFLTCYBERCOM is authorized direct liaison authority with NAVCYBERFOR for collaboration and coordination of MTE support.

f. Reserve Units. Navy Reserve units are aligned to, and integrated with, specific COMFLTCYBERCOM Active Component (AC) commands. The supported AC Commanding Officer will operationally employ the assigned reserve units.

g. Joint Assignments

(1) COMFLTCYBERCOM is the NCC to USSTRATCOM for cyberspace operations, space operations and IO, and the Navy Cyber Component Commander to USCYBERCOM.

(2) COMTENTHFLT is the numbered fleet commander assigned to USSTRATCOM for cyberspace operations, space operations, and IO. COMTENTHFLT reports operationally to COMFLTCYBERCOM.

(3) FLTCYBERCOM forces assigned to USSTRATCOM are drawn from task forces and commands organized under TENTHFLT's task organization per section 1053 of reference (e). These task forces and commands report operationally to COMTENTHFLT.

h. Support Relationships and Coordinating Authority

(1) The overarching relationship between COMFLTCYBERCOM and each NCC and echelon 2 commander in the Navy is mutual support, which requires frequent and close collaboration and coordination to successfully execute and prioritize their respective missions. The supported and supporting command relationship varies depending on the mission area and specific tasks to be performed by COMFLTCYBERCOM and the other commander.

(2) As the central operational authority for Navy networks, COMFLTCYBERCOM is the supported commander for networks and, as such, exercises centralized control for planning and execution of all NETOPS and defensive actions on Navy networks. FLTCYBERCOM is the supporting commander for providing NCCs and other echelon 2 commanders a secure, reliable and available network capability.

(3) COMFLTCYBERCOM and COMTENTHFLT have coordinating authority with Navy operational commanders to establish Navy operational requirements as the operational lead for cyber, cryptology and SIGINT, IO, EW, and space.

(4) COMFLTCYBERCOM has coordinating authority with all NCCs for the planning of cyberspace operations, IO, EW, space operations, and cryptologic and SIGINT operations in support of operational plans and contingency operations.

(5) COMTENTHFLT has coordinating authority with all numbered fleet commanders concerning cryptologic operations to include planning, tasking and the allocation of resources to support cryptologic operations.

(6) COMTENTHFLT has coordinating authority with all numbered fleet commanders regarding COMTENTHFLT mission areas.

i. Space and Naval Warfare Systems Command (SPAWARSYSCOM). COMFLTCYBERCOM coordinates with SPAWARSYSCOM on research and development (R&D), procurement of capabilities, technical support, and SPAWARSYSCOM's other responsibilities under reference (f).

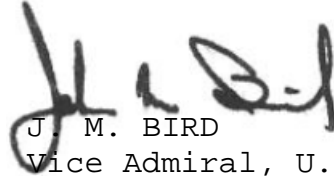
## 6. Action

a. In accomplishing assigned missions, COMFLTCYBERCOM and COMTENTHFLT shall perform the functions and tasks in enclosure (1). COMFLTCYBERCOM and COMTENTHFLT shall submit recommended changes and revisions to this instruction when required.

b. If anything in this instruction later becomes inconsistent with a higher authority (Department of Defense (DoD), Navy, joint, intelligence community) or other applicable directive or regulation, the higher authority directive or regulation shall be followed.

OPNAVINST 5450.345  
04 April 12

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of January 2012.



J. M. BIRD  
Vice Admiral, U.S. Navy  
Director, Navy Staff

Distribution:

Electronic only, via Department of the Navy Issuances Web site  
<http://doni.daps.dla.mil>





FUNCTIONS AND TASKS OF COMFLTCYBERCOM AND COMTENTHFLT

COMFLTCYBERCOM and COMTENTHFLT operationally control all FLTCYBERCOM and TENTHFLT forces. COMFLTCYBERCOM may delegate appropriate missions, functions and tasks to COMTENTHFLT and subordinate commands.

1. Cyberspace Operations, Network Management and Inspections.  
COMFLTCYBERCOM:

a. Serves as the central operational authority for Navy networks. As the central operational authority, COMFLTCYBERCOM is responsible for developing the requirements for, and directing the operations, maintenance, security, defense, and integration of the Navy's portion of the GIG.

(1) COMFLTCYBERCOM dynamically and proactively manages network throughput, rapidly responds to network anomalies, and defends the networks through the use of actions that may include, but are not limited to: record message MINIMIZE, blocking of network ports and protocols, and unit quarantine. While unilateral operations are not expected to be routine, CNO delegates authority and responsibility to COMFLTCYBERCOM to take unilateral action in appropriate circumstances on Navy networks. This authority will be exercised with due consideration for the operational impact on other commanders and their subordinate forces, and when possible will be exercised only after COMFLTCYBERCOM coordinates with the affected echelon 2 commander, or that commander's designee, to conduct an operational risk assessment on those actions that could limit the operational capabilities of the affected commander. Echelon 2 NCCs will normally delegate this authority to a numbered fleet commander that has operational control of the affected unit. If coordination cannot occur before taking an action with potential operational impact, COMFLTCYBERCOM will provide information on the action taken as soon as practical.

(2) COMFLTCYBERCOM is responsible for centralized command and control (C2), operation, and management of the Navy's networks and has sole authority to set standards for network security, operational performance, compliance, configuration control, accreditation, and certification and is responsible for delivering a global Navy cyber network common operational picture.

(3) COMFLTCYBERCOM exercises operational authority to safeguard the interface between Navy networks and those network elements that perform combat and weapon system, fire control, flight, and hull, mechanical and electrical control functions.

(4) COMFLTCYBERCOM ensures Navy network compliance with Federal law and DoD, joint, and Navy directives.

(5) COMFLTCYBERCOM ensures Navy networks provide the capability to respond to joint, coalition, Navy component, and fleet commander mission requirements.

b. Serves as the Navy cyber component commander to USCYBERCOM.

c. Serves as the designated approval authority (DAA)/AO for assigned networks and carries out the responsibilities under DoD Instruction 8510.01 of 28 November 2007.

(1) Serves as the ODAA/AO for collateral and general services, classified and unclassified, information systems, networks, and telecommunications systems per reference (f).

(2) Serves as the DAA/AO for any additional networks and information systems identified by CNO.

d. Operates the Navy's tier 2 computer network defense service provider, per reference (f) and DoD Directive O-8530.1 of 8 January 2001.

e. Plans, coordinates, synchronizes, deconflicts and executes Navy cyberspace operations.

f. Maintains and shares situational awareness of the Navy's portion of the GIG.

g. Directs the Navy's cyberspace operations Red Team. The Red Team conducts penetration testing and vulnerability analysis during exercises and as required.

h. Directs the Navy's cyberspace operations Blue Team. The Blue Team conducts vulnerability network assessments.

- i. Directs and manages the Cyber Security Inspection and Certification Program for the Navy.
- j. Implements the responsibilities assigned in DoD, joint, and Navy information assurance, NETOPS, network defense and cyberspace related instructions.
- k. Provides network transport for NCC and numbered fleet maritime operations centers (MOCs) as well as advice and assistance on issues pertaining to NETOPS. The C2 and coalition systems used by each individual MOC will be maintained by the respective NCC and numbered fleet.
- l. The single process owner for the Naval NETWAR FORCENet Enterprise.
- m. Ensures FLTCYBERCOM command information officer (CIO) coordination with other echelon 2 CIOs on fleet operational information management and information technology capabilities.
- n. Serves, with COMPACFLT and COMUSFLTFORCOM, as co-chair of the Functional Area Manager Fleet Application Steering Group. As part of those responsibilities, coordinates with other co-chairs to determine appropriate decision criteria for fleet applications and systems and provides guidance regarding application impacts on overall network performance and security posture.
- o. Conducts command cyber readiness inspections on Navy units, commands, and installations as directed by USCYBERCOM.

2. IO and EW. COMFLTCYBERCOM:

- a. Directs and manages the IO direct support augmentation program. Provides force and equipment allocation to augment fleet capabilities based on NCCs and numbered fleet stated operational information or effect requirements. Capabilities may be comprised of a combination of forward deployment of personnel, carry-on equipment, and or shore-based support.
- b. Supports IO and EW capability planning requirements and target development through capabilities analysis against NCC and numbered fleet overarching plans and associated joint target lists (JTL).

c. Coordinates and administers the Navy OPSEC program, including web risk assessment, and provides oversight regarding the execution of Navy OPSEC policy, doctrine, instruction and organizational program implementation, per OPNAVINST 3432.1A.

d. Assumes responsibilities for managing and coordinating EW system programming through EW data production and maintenance for fleet operations and air, subsurface and surface platforms per OPNAVINST 3430.23B.

e. Coordinates the annual review of Navywide operations tasks (OPTASK) related to COMFLT CYBERCOM and COMTENTHFLT mission areas for submission to the OPTASK flag review panel.

f. In coordination with the NCCs, develop consolidated fleet IO and EW gap issues and associated requirements for submission to the Office of the Chief of Naval Operations (OPNAV) resource sponsors.

g. Coordinates fleet R&D requirements and facilitates R&D activities for IO and EW.

h. Serves as the Navy's lead for operational and tactical EW issues.

i. Responsible for ensuring fleet units are compliant with spectrum management policy and guidance.

3. Cryptologic Operations and Intelligence. COMFLT CYBERCOM is the central operational authority for cryptologic operations.

a. COMFLT CYBERCOM serves as the Navy's SCC commander to DIRNSA/CHCSS. The SCC serves as the primary Service authority for all operations, programming, budgeting, training, personnel, policy, doctrine, and foreign relationships for cryptologic activities. The SCC commander is also responsible for the development of strategic plans, policy, processes, requirements, architectures and communications.

b. COMFLTCYBERCOM directs and tasks the operations of its subordinate cryptologic commands to include providing cryptologic support to NCCs and numbered fleets.

c. In appropriate circumstances, COMTENTHFLT and another numbered fleet may agree to shift primary tasking authority of a specific unit or unit's sensors to the other command for a specified duration of time.

d. COMFLTCYBERCOM directs and manages the Cryptologic Direct Support Augmentation Program. This includes determining force and equipment allocation of direct support equipment and personnel based on NCC numbered fleet stated operational information or effects requirements. These capabilities may be comprised of a combination of forward deployment of personnel, carry-on equipment, and or shore-based support.

e. COMFLTCYBERCOM and COMTENTHFLT direct task forces and commands to support the intelligence and target development requirements of USSTRATCOM, USCYBERCOM, joint force commanders, and naval commanders in support of fires and effects planning.

f. COMFLTCYBERCOM and COMTENTHFLT generate intelligence requirements in support of FLTCYBERCOM and TENTHFLT mission sets.

g. COMFLTCYBERCOM serves as the intelligence oversight program manager for FLTCYBERCOM units and Navy units for which it sponsors specialized database access. COMFLTCYBERCOM ensures intelligence oversight reports for these units are consolidated and submitted to the Navy Inspector General and the respective database owner. COMFLTCYBERCOM will keep NCCs and numbered fleets informed of any non-compliance with intelligence directives.

h. COMFLTCYBERCOM and COMTENTHFLT maintain Navy cryptologic liaisons at appropriate combat support agencies.

i. COMFLTCYBERCOM and COMTENTHFLT provide support and technical guidance to Navy operating forces on cryptologic matters, to include fielding of approved capabilities.

j. COMFLTCYBERCOM oversees the direction and modernization of the Navy's cryptologic architecture.

k. COMFLTCYBERCOM serves as a member of the Five Eyes Maritime Cryptologic Committee in support of CNO (N2/N6), the designated U.S. Navy lead.

l. COMFLTCYBERCOM is the Navy's critical information program manager.

4. Space. COMFLTCYBERCOM is the central operational authority for Navy space activities. COMFLTCYBERCOM:

a. Serves as the NCC to Commander, U.S. Strategic Command (CDRUSSTRATCOM) for Navy space operations. As part of that responsibility, advises USSTRATCOM, including its subordinate command, the Joint Functional Component Command for Space, on global operations that may be impacted by theater support requirements.

b. Maintains and operates assigned satellite systems, ground stations, and associated equipment.

c. Provides specialized satellite communications (SATCOM) forces and resources to conduct operations in support of the Global SATCOM Support Center and Regional SATCOM Support Centers.

d. Maintains a space operations cell to provide intelligence, space planning, and space effects packages; MOC planning and execution support; and carrier and expeditionary strike group and amphibious ready group space support, analysis and assessment.

e. Coordinates with the Navy Tactical Exploitation of National Capabilities (TENCAP) Program Office to ensure fleet needs are identified and addressed through appropriate R&D efforts. Manages FLTCYBERCOM delegated TENCAP requirements through liaison with Navy TENCAP field offices.

5. Planning and Fires. COMFLTCYBERCOM and COMTENTHFLT:

a. Direct TENTHFLT task forces and commands to support the intelligence and target development requirements of USSTRATCOM, USCYBERCOM, joint force commanders, and naval component commanders in support of fires and effects planning.

b. Support USSTRATCOM, USCYBERCOM, joint force commanders, and naval component commanders contingency and crisis action planning as directed.

c. Execute USSTRATCOM and USCYBERCOM operations, including coordination with other joint, Navy, and multinational commands, as directed by CDRUSSTRATCOM and Commander, USCYBERCOM.

d. Support capability planning requirements related to COMFLTCYBERCOM and COMTENTHFLT mission areas through capabilities analysis against joint, NCC and numbered fleet overarching plans and associated JTLs.

e. Review Navy, joint, allied and coalition plans and policies to include general and contingency plans. Develop, as appropriate, IO, EW, cyberspace, cryptologic and SIGINT and space concept of operations (CONOPS).

f. Assign, direct, and apportion TENTHFLT task force fires elements as directed by USCYBERCOM.

g. In support of the Charter for the Integrated Broadcast Service Support Office (IBSSO) of 3 January 2001 serve as Navy's designated operational manager for the integrated broadcast service capabilities. Provide direction and oversight of the IBSSO.

6. Exercises and Fleet Readiness Training Plan (F RTP).  
COMFLTCYBERCOM and COMTENTHFLT:

a. Define and provide F RTP and 7th Fleet Training Plan (7FTP) Integrated, Advanced and Sustainment Phase training completion criteria and certification standards for COMFLTCYBERCOM and COMTENTHFLT mission areas.

b. Execute F RTP and 7FTP Integrated, Advanced and Sustainment Phase training and certification actions for COMFLTCYBERCOM and COMTENTHFLT mission areas.

c. Provide support for Navy, joint, and multinational exercises and F RTP and 7FTP events within COMFLTCYBERCOM and COMTENTHFLT mission areas and resource constraints.

d. Support fleet experimentation and exercise requirements within COMFLTCYBERCOM and COMTENTHFLT mission areas.

7. Communications Security (COMSEC). COMFLTCYBERCOM:

a. Carries out the responsibilities previously assigned to NAVNETWARCOM in OPNAVINST 2201.3B.

b. Coordinates COMSEC monitoring for the fleet.

c. Provides advice and assistance to the CNO regarding the conduct of COMSEC monitoring activities and procurement of COMSEC monitoring resources.

8. Requirements, Budget, and Capabilities Development.

COMFLTCYBERCOM will carry out the following responsibilities:

a. Develop, coordinate with the other NCCs, prioritize, and articulate to the CNO the Navy's operational requirements for cyber, space, and cryptologic capabilities, to include SIGINT capabilities associated with and in support of EW, following the Planning, Programming, Budgeting, and Execution System process and timelines.

b. Develop, coordinate with the other NCCs, and prioritize the Navy's operational requirements for EW and IO capabilities, other than cyber capabilities, and provide them to COMUSFLTFORCOM for integration with fleet warfighting capability requirements and submission to CNO.

c. Collaborate with COMUSFLTFORCOM to ensure cyber, IO, cryptologic and SIGINT, space operations and C2 capabilities Navy mission essential tasks are appropriately documented and tracked in the Navy Training and Information Management System (NTIMS).

d. Carry out the responsibilities of BSO 60C.

e. Administer FLTCYBERCOM resource management systems and prepare operating budget estimates for assigned shore activities. Present and defend budget estimates and collaborate with other commands and offices concerning the provision of



financial resources. Review resource usage and prepare and issue progress reports to higher authority as directed or required.

f. Oversee electronic and cyberspace capabilities certifications processes.

g. Direct rapid capabilities development and technology insertion.

h. Direct and coordinate the development of capabilities related to COMFTLCYBERCOM and COMTENTHFLT mission areas to support military operations.

i. Direct resource decisions, including manpower, for applicable FLTCYBERCOM operations, missions and functions and for resources identified as supporting assigned missions and lines of operations.

j. Conduct large-scale experimentation, individual demonstration projects, and limited objective experiments Navywide. Develop and implement cross-domain, multinational solutions.

k. Develop and integrate innovative technologies into Navywide experiments and other appropriate warfare exercises to ensure that tactics, techniques and procedures (TTPs) are developed in support of these technologies. Lead development of fleet science and technology needs at appropriate forums.

l. Responsible for the management of command, control, communications, computers, combat systems, intelligence, surveillance, and reconnaissance (C5ISR) modernization required to maintain strike force and C5ISR interoperability across naval, joint, and coalition environments. Per COMUSFLTFORCOMINST 4620.3B and COMPACFLTINST 4620.3B (NOTAL), participate as a major stakeholder of the Navy C5ISR Modernization Conference in COMFLTCYBERCOM's role as central operational authority of Navy networks.

m. Participate as a major stakeholder in coalition and allied network interoperability forums (e.g., Multinational Maritime Internet Protocol Interoperability Conference and

Military Cooperation Commission) in order to unify coalition and allied network interoperability efforts across all classification domains.

n. Coordinate and assess operational utility of materiel solutions within assigned mission areas that affect fleet capabilities.

9. CONOPS, TTPs and Doctrine. COMFLTCYBERCOM:

a. Coordinates development of CONOPS related to COMFLTCYBERCOM and COMTENTHFLT mission areas with COMUSFLTFORCOM and COMPACFLT.

b. Coordinates development of doctrine related to COMFLTCYBERCOM and COMTENTHFLT mission areas with Navy Warfare Development Command.

c. Ensures uniformity of TTPs across the fleet in COMFLTCYBERCOM and COMTENTHFLT mission areas.

d. Leads Navywide exercise and experimentation to advance technology development and integration, and development of doctrine and TTPs related to COMFLTCYBERCOM and COMTENTHFLT mission areas.

e. Advocates for funding of warfare centers of excellence managed by subordinate commands.

10. Telecommunications. COMFLTCYBERCOM:

a. Manages shore telecommunications services.

b. Directs sustainment of Navy teleport and SATCOM (super high frequency, extremely high frequency, mobile user objective system, commercial wideband SATCOM program, Navy multiband terminal) capabilities.

c. Directs sustainment of Navy transport services, including automated digital network system, piers, and high frequency.

- d. Directs sustainment of telecommunications support for:
    - (1) MOCs
    - (2) Ballistic missile defense shore
    - (3) Submarine communications
    - (4) Defense Red Switch Network
    - (5) Navy circuit management
    - (6) Base communications
    - (7) Telephony
  - e. Supports Navy interests and equities in joint plans and theater joint tactical network.
  - f. Provides representation to the C5I Modernization Configuration Management and Theater Enterprise Computing Center Central Region and Military Construction boards.
11. Readiness and MTE Functions. COMFLTCYBERCOM:
- a. As the designated commander of the Navy's SCC, COMFLTCYBERCOM is responsible for MTE functions of the Consolidated Cryptologic Program funded cryptologic workforce, per reference (c). This MTE responsibility also extends to cryptologic activities funded through General Defense Intelligence Program and executed by FLTCYBERCOM headquarters and subordinate operational commands. COMUSFLTFORCOM, via NAVCYBERFOR, the global C5I type commander, provides MTE functions for all cyber forces afloat and ashore to generate required levels of current and future force readiness.
  - b. Prioritizes mission area manpower requirements, including, but not limited to direct support submarine, air, and surface; EW; computer network attack, exploitation, and defense; NETOPS; information assurance, space; and fleet electronic support.
  - c. Assesses Navy cyber readiness.

d. Per OPNAVINST 3501.360, identifies, reviews and ensures operational capabilities for fleet readiness and exercise requirements are being met. Ensures fleet commanders are assessing and developing mission area requirements; Defense Readiness Reporting System - Navy (DRRS-N) conditions and standards; and assessment criteria specific to their operational areas that adequately prepare forces for operational exercises and mission tasks.

e. Coordinates with Commander, Naval Education and Training Command and the fleet training groups to provide operational training requirements and ensure standardization and completeness in the training curricula related to COMFLTCYBERCOM and COMTENTHFLT mission areas.

12. Security. Per DoD 5105.21.M-1, Department of Defense Sensitive Compartmented Information Administrative Security Manual, August 1998; SECNAV M-5510.30 of June 2006; SECNAVINST 5510.30B; SECNAV M-5510.36 of June 2006; and SECNAVINST 5510.36A, COMFLTCYBERCOM and COMTENTHFLT manage and oversee all aspects of physical, personnel and traditional information security for the COMFLTCYBERCOM domain, and all cryptologic personnel regardless of assignment, following the standards as set forth in Executive Order (E.O.) 12968, Intelligence Community Directive 704, Intelligence Community Directive 705, DoD Instruction 5200.01 of 9 October 2008, DoD Directive 5200.2 of 9 April 1999, and DoD 5105.21.M-1, Department of Defense Sensitive Compartmented Information Administrative Security Manual, of 1 August 1998. Exercise original classification authority for the COMFLTCYBERCOM domain per the standards as set forth in DoD 5200.1-R, Information Security Program, of 14 January 1997, and operate the DON Personnel Security Interview Program operated out of the COMFLTCYBERCOM field office, Recruit Training Command Great Lakes per DoD 5200.2-R, Personnel Security Program, of 1 January 1987.