COE - Maritime Management Plan

(This page is intentionally blank)

Table of Contents

1. Purpose of Plan

2. Maritime COE Process and Migration to Network Centric Enterprise Services (NCES)

   A. Overview of COE Process and Infrastructure for Maritime Customers

   B. Migration to Network Centric Enterprise Services (NCES)

3. Financial Process for Support of COE for Maritime Customers

Appendices

Appendix A: COE-Maritime Contact Information

Appendix B: List of Applicable Websites

Appendix C: References

Appendix D: Key Roles and Responsibilities

Appendix E: COE-M Management Board

Appendix F: Maritime Configuration Control Board

Appendix G: COE AOG and TWGs

Appendix H: COE-M Subscriber Support Services

Appendix I: COE Compliance

Appendix J: COE-M Software Change Request (SCR) Process, Segment Registration, and Software Distribution

Appendix K: COE License Requirements and Management

Appendix L: Maritime Extensions

Appendix M: Engineering Change Proposal (ECP) Format

Appendix N: Acronyms and Definitions

Appendix O: Limited Release Agreement

Appendix P: GCCS-M POC and MOA Information

(This page is intentionally blank)

1. Purpose.

This document provides basic guidance for the management of the Common Operation Environment (COE) by PEO C4I & Space ("PEO C4I" for short and formerly SPAWAR PD-15), the Navy's Executive Agent (EA) for the COE. This guidance includes necessary technical, organizational, and financial processes required for maritime users hereto referred to as Subscribers, to successfully migrate to and develop upon the COE. Maritime subscribers to the COE encompass programs/systems from all the naval SYSCOMs, USCG programs, some USMC programs, and Maritime directed Joint programs. This plan will be updated on an annual basis in order to keep pace with the evolving COE process.

Note that throughout this plan, COE (or COE-M, as the maritime use of COE is referred) and GCCS-M are utilized but they are not synonymous. COE-M and GCCS-M, though they are two distinct and separate entities, they are often used incorrectly/interchangeably. COE-M is the infrastructure/foundational software on which maritime programs build their systems. GCCS-M, managed by SPAWAR PMW-157, is the largest COE-M subscriber program and was the first program to field a COE based system. It should be noted, however, that GCCS-M is treated and participates equally in the COE-M process with other maritime subscribers. Since GCCS-M is, however, the most prevalent COE based system in the Navy today, many programs/system developers desire to integrate their COE based system/segments/capability within GCCS-M's COE based architecture. GCCS-M software/services are NOT covered by one's COE-M subscriber's status/agreement. GCCS-M software/segments must be coordinated directly with PMW-157. To aid COE-M subscriber programs, PMW-157/GCCS-M point of contact and MOA information are provided in Appendix P of this document.

2. Maritime COE Process and Migration to Network Centric Enterprise Services (NCES)

A. Overview of COE Process and Infrastructure for Maritime Customers

The COE concept contains the fundamental building blocks and architecture for DoD C2/C4I systems and defines an approach for building interoperable systems by specifying guidelines and standards by which the Services can reuse common existing software components and properly build new software in a seamless, automated fashion. This approach takes full advantage of the use of proven Commercial-Off-The-Shelf (COTS) products to the maximum extent possible and utilizes standard commercial Operating Systems (OS). The standard COE architecture is depicted in Figure-1. In this architecture, COE provides the C4I "core" software (including the Application Programmer Interfaces [API] layer) and then mission applications are developed as segments by system developers using the API's. DISA maintains and evolves COE and provides products to a single point of contact in each service (Navy also handles distribution to USCG), which in turn distributes and supports COE for customers within their respective service. The single point of contact in Navy, as previously indicated is PEO C4I. The DISA COE process includes a joint Configuration Management (CM) and engineering process that is described in Appendices E and F.

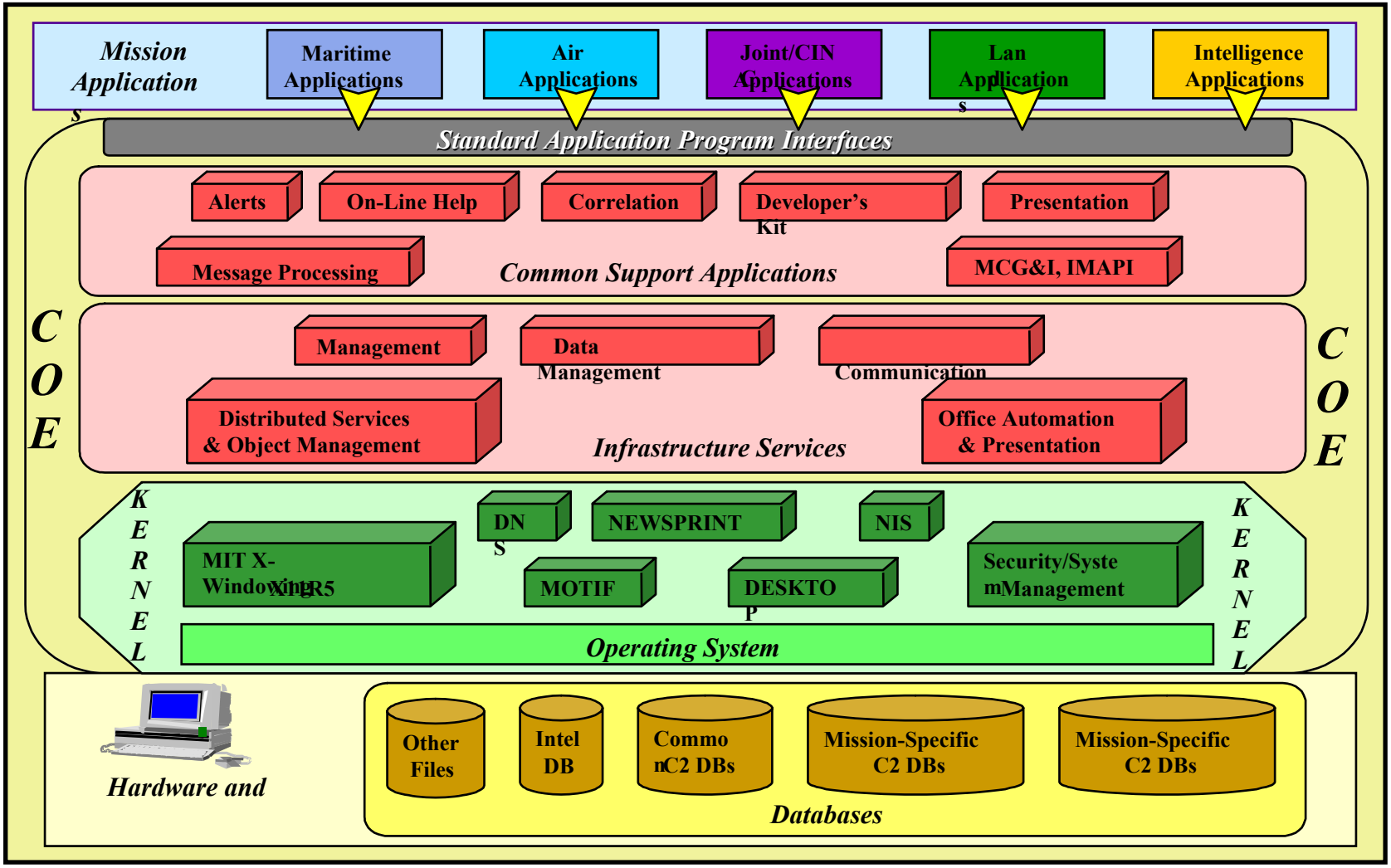

Figure-1: COE Architecture

The Navy EA maintains an infrastructure for supporting maritime customers as shown in Figure-2.

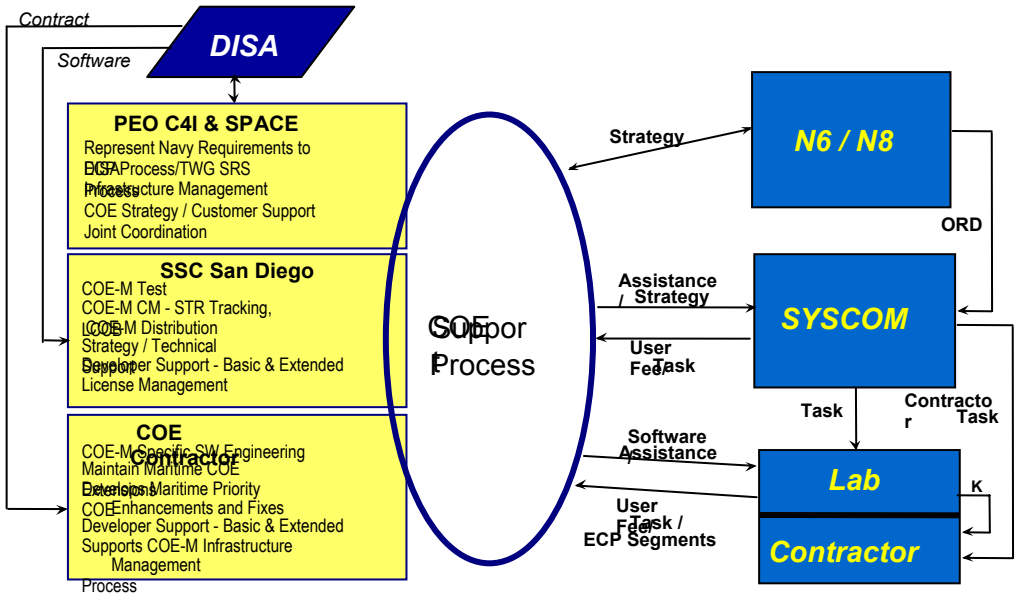

Figure-2: Customer Support Process

As implied in the preceding diagram, the Navy EA executes four primary functions:

A. COE Requirements Process and coordination with DISA
B. COE Software Support Activity (SSA), including COE software testing, configuration management, distribution, and tracking of COE software trouble reports/change proposals (STR/SCP).
C. COE technical support to maritime customers
D. Development and maintenance of maritime components/extensions (maritime support applications/segments required by maritime customers as a whole but not of "joint" applicability and therefore not under DISA's charter to absorb/maintain (see Appendix L for details).

Though utilization of the COE will ensure significant reduction in both developmental and life cycle cost and greater interoperability with other COE based systems, development on and/or migration to the COE can initially be a challenging endeavor. For this reason, the Navy EA has established a COE-M Customer Support Team (CST) that is chartered to assist programs in their migration to the COE and/or development of new systems on the COE. Besides the "technical" issues regarding utilization of the COE, a significant part of the effort is to fully understand what system requirements are satisfied by the COE, which can be satisfied by modifying the COE, and which are program/system specific requirements that must be developed as mission applications/segments. In the past, the program and it developers for the most part did this with little, if any, outside assistance. In some cases this "go it alone" approach was successful, however, more often it has lead to incorrect assumptions that influenced architectural or implementation

decisions that have resulted in unnecessarily complicated implementations and/or system requirements not being adequately satisfied. The primary focus of the CST is to ensure the above does not occur and that all COE-M subscribers are successful in their implementation of the COE. As such, Figure-3 below depicts the engineering process

To summarize, COE and COE based systems consist of the following components:

- **DISA-provided COE and development environment** (Supported/distributed under this plan)
- **COE-M maintained Maritime Extensions** (Supported/distributed under this plan)
- **Operating Systems and Licensed COTS COE products**
  - The Operating Systems and version thereof, differ depending on the COE version, however, they are always standard COTS versions. It is the responsibility of the system developer to acquire the necessary operating system license and, if desired, to apply appropriate OS patches provided via DISA.
  - COE supports a number of licensed COTS products such as MICROSOFT OFFICE, SYBASE, ORACLE, NETMEETING, etc. DISA packages many of these into COE compliant segments for each COE version and they are available to subscribers who have the appropriate licenses. While a few of the COTS segments are provided under COE-wide Enterprise licenses (e.g., NETSCAPE), most require the subscriber to have a valid license and it is COE-M SSA's responsibility to validate that customers are in possession of the appropriate licenses prior to shipping COTS software. See Appendix K for details on license requirements and management.

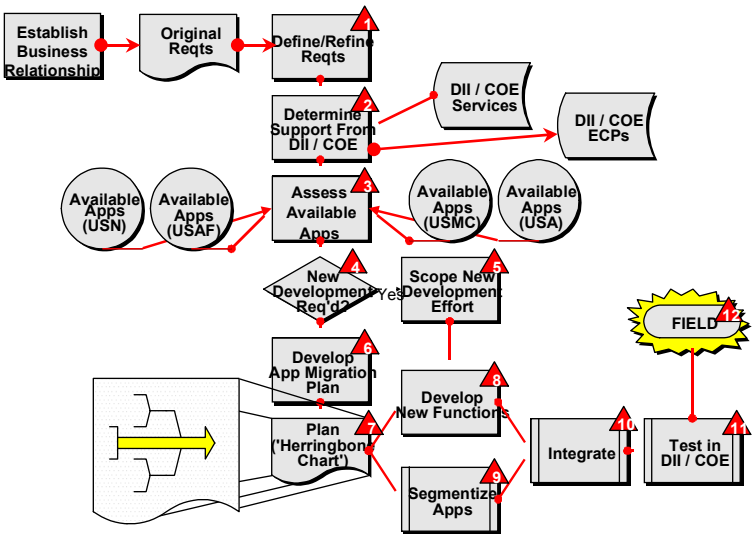

Figure-3: DII COE Systems Engineering Process

- **Mission Application Segments** not directly covered under this plan subscribers should coordinate directly with the appropriate program office. For GCCS-M segments, the PMW-157 points of contacts provided Appendix P of this document. In the case of "Joint" mission applications, the Navy EA can provide POC information on request

B. Migration to Network Centric Enterprise Services (NCES)

Currently the COE is not an "official program" in that it does not have a designated budget line of it's own (DISA funds COE out of it's overall budget). Due to the problems associated with this obviously sub-optimal situation, OSD/C3I initiated an effort to make COE a officially designated program with it's own funding line. As this initiative progressed, OSD has renamed the program Network Centric Enterprise Services (NCES), broadening it's scope to better align with technology and move to a more network centric environment using a set of core enterprise services. In essence, NCES is the initial step to the implementation of the Global Information Grid (GIG) (depicted in Figure 4 below). Accordingly, what began as COE, is now moving forward as a proposed ACAT-1 NCES program, with today's COE foundation being a key element. At the writing of the document, specific details regarding NCES are not known, but the following can be said:

- The current 4.X COE infrastructure will be a foundational element and basis for the NCES supported common operational picture (COP)
- While moving to a network centric environment, it is realized that NCES will have to continue to support the current platform centric implementations.
- NCES will be incrementally implemented with initial versions adding enterprise services over the current COE foundation; the initial NCES version 1.X targeted for early FY05.

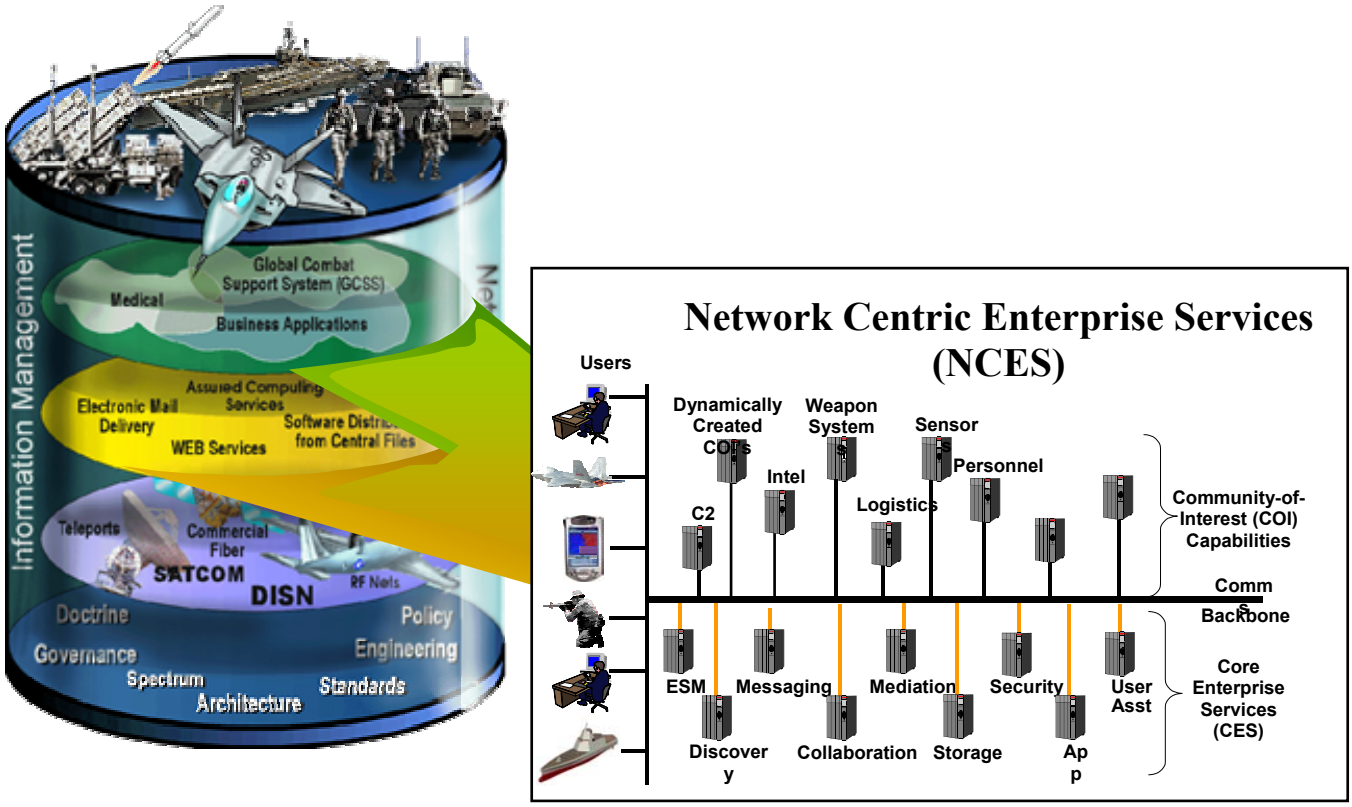

Figure 4: NCES – the Enterprise Services for the Global Information Grid (GIG)

3. Financial Process for Support of COE for Maritime Customers

The Maritime COE infrastructure and processes supported by the Navy EA cost approximately $5+M annually to execute. The functions of the Navy EA are funded through a combination of an OPNAV (N62) program line (about $1.5M) and subscriber program user fees. The fees are designed to fair-share the infrastructure costs across the programs, as well as reflect the benefit derived from COE. The fee structure addresses established maritime programs of record, Foreign Military Sales (FMS) programs, Non-Tactical programs only requiring the kernel and selected run-time segments, Independent Research and Development (IR&D), the Request for Proposal (RFP) process, Advanced Concepts activities, and programs conducting initial investigation into the use of the Maritime COE. This fee structure is evaluated on a yearly basis and is open to constructive input as to how to improve it.

A. Basic Fee Structure for Maritime Developers

Maritime customers share the below fee structure:

Fee per developer: $50K
User Base Fee
- $25K for 1 to 4 fielded sites (small)
- $50K for 5 to 14 fielded sites (medium)
- $75K for 15 or more fielded sites (large)

Under the above structure, a “developer” is defined as a separate programmatic or technical software development effort/location. Accordingly, a program/system may have more than one developer and many separate development sites, with each being considered a “separate developer”, though it may be the same contractor. A given contractor may have more than one “development effort” for a given program without an additional charge. However, a specific contractor/developer may not develop software for another program unless it is a designated developer for that program (i.e., the program is a subscriber and pays the appropriate developer's fee).

The User Base Fee (often called “Site” fee) is derived from the number of fielded sites, with a fielded site being defined as an operational installation. The purpose of this user base fee is to help fund resolution of STR’s and SCP’s resulting from operational use and also to pro-rate the cost of the COE infrastructure across programs that are benefiting from the reduced life cycle cost associated with COE. When a program/system has a “prime contractor” responsible for the development, integration, and delivery of the system, the prime contractor is responsible to ensure that all sub-contractors participating in any development efforts requiring use of the COE development environment, are registered as developers for the program and the appropriate developer fees are paid. Again, if contract XYZ is a registered developer for a given program, the development environment is only “licensed” for that program, thus any development for additional programs require a new development fee (license).

Foreign Military Sales (FMS) cases through the Navy are levied COE subscriber fees that follow the same guidelines established for other subscribers. FMS cases for GCCS-M are levied a COE-M site fee to cover a fair share of the COE development and maintenance costs and those cases also desiring to develop COE based applications incur the appropriate developers fee. Note that COE,

and therefore COE-M, are not themselves directly releasable. Releasability for programs of record is managed by the Foreign Releasability Board (FRB) and once given COE based program has been approved for foreign release and a FMS case has been established, the COE itself is considered "released".

Each August, the BFM will send a "FY-XX Subscribers Fee" letter/email to all current and anticipated COE-M subscribers for the next fiscal year to baseline the subscriber programs and determine the projected budget available fund the COE-M support infrastructure. These letters will provide the various points of contact for each subscriber program, list all the program developers, and provide the subscribers fees for the next year based on the listed developers. Each subscriber program will be asked to validate/update the point of contact and developer information and to acknowledge their agreement with the stated subscribers fee.

For customers that require support above and beyond that covered under the basic services, a direct support task may be negotiated with the Navy EA BFM for services. Appendix H provides a list of the basic support service and also additional services that are available under an "extended plan".

B. Limited Release Fee Structure for IR&D/RFP/Evaluation/Advance Concepts Activities

A Limited Release Option (LRO) has been established to accommodate COE users that meet one of the below criteria:

- those that are interested in investigating the potential use of the COE for their program ;
- activities which are interested in either "getting smart" regarding the use of or for doing IR&D efforts with the COE;
- programs and or activities participating in the proposal process;
- government activities who are involved in advance concept/R&D efforts and that would benefit by using the COE to support eventually transition to the fleet;
- programs only requiring the COE Kernel, segmented COTS products, and possibly limited GOTS segments.

To support these requirements, the following options are provided:

- <u>One-time Evaluator's Option:</u> Fee is $5,000 per release.
  This provides a one-time delivery of a requested development environment (software and available softcopy documentation) to the designated activity and 5-hours of telephone support during the first two weeks after COE delivery to address installation issues and or basic development environment questions. Completion of a Limited Release Agreement (Appendix O) will be required.

- <u>Expanded Evaluator's Option:</u> Fee is $10,000 per FY.
  In addition to what is provided by the "One-time Evaluator's Option", this option provides access to all distributed updates to the development environment for the remainder of the fiscal year. Completion of a Limited Release Agreement (Appendix O) will be required.

- IR&D Option: Fee is $20,000 per FY.
  This option provides all updates to the COE development environment and download access from COE segments from the COE-M website, plus limit additional technical support above that in the Evaluator's Options. As with the LRO, an "IR&D Agreement" will be required which specifically defines their intended use of the COE, that no further distribution is authorized, and that if any resultant IR&D effort if fielded/goes operational, the remainder of standard developers fee (an additional $30,000) will be accessed. Completion of a Limited Release Agreement (Appendix O) will be required.

- RFP Option: Fee is a standard developer's fee ($50,000) plus $5,000 per developer per FY.
  This is specifically designed for programs participating in a RFP process. This option provides the development environment and updates for the remainder of the FY and the basic level of support discussed in Appendix H, however, requires that all software distribution and support be "funneled" through a designated government representative of the program in order to ensure all candidates are provided equal access to information.

- Advance Concepts Option: Fee is $10k per project per FY.
  This is specifically designed for activities such as ONR and other maritime activities that are involved in developing new leading edge concepts/ prototypes. Use of the COE software foundation both facilitates the developmental process and provides a means to easily productize successful development efforts and expedite fleet release/introduction. Under this option, the qualifying activity will be required to establish a single point of contact/technical interchange who will be the sole interface between the COE office and the activities developers. This will provide access to the COE development environment and all updates on a project-by-project basis. The activity will be required to provide a list all efforts being supported and the developers (max of 2 per project) who will receive the software (either directly for SSA or through the activities central POC).

- Kernel Option: Fee is $15k per project per FY.
  This is targeted for programs (primarily non-tactical) that do not require the C4I development environment and who plan to only use the COE Kernel, segmented COTS products, and possibly limited GOTS segments. This access is provided for up to two activities with $5k charge for each additional two activities/developers.

C. Special Case/Negotiated Fees

While the majority of the subscribers will fall under either the Basic or the LRA category, there may be special situations that warrant the fees to be negotiated (one such case is the JMPS program and their related UPCs). These special cases will be handled on a case-by-case basis and coordinated between the program and the COE-M Manager.

D. Financial Mechanics

COE-M funding and contractual related matters are handled by the COE-M Manager and the Financial Assistant (contact information in Appendix A). In general, fees and funding associated

with the above financial process do not come into a common account from which they are distributed. Instead, the Financial Assistant will coordinate with individual customers to direct their fees to the appropriate executing/support activity. The most common funding documents used are: Request for Contractual Procurement (RCP), Work Requests (WR/WX), or Military Interdepartmental Purchase Requests (MIPR). These funding documents do vary for the different subscriber programs. In order to ensure that the funding documents are sent to the correct place in the right format, it is critical that the COE-M Manager or Financial Assistant be contacted for coordination "**prior to"** funds being issued. The following are examples of funding documents from various commands:

From	To SPAWAR	To SSC-SD
Navy Headquarters	RCP	WX
Navy Field Site	RCP	WX
USCG	MIPR	MIPR
USMC/Other	RCP or MIPR	WX or MIPR

The preferred appropriations for COE development and maintenance by the COE program office are Research and Development (R&D), Operations and Maintenance (O&M), or Foreign Military Sales (FMS). Other Procurement, Navy (OPN) is allowable, although NOT preferred because it is more difficult to execute this funding type based on the COE scope of work. In addition, other forms of funding are very difficult to get on task with the various developers and life cycle managers of the COE development team.

A sample of a statement that might be used under the funding document's work description would be "Funds are provided for COE-M User Fees in support of Program XXX."

Appendix A contains details as to where to send COE-M funding documents.

All COE-Maritime subscriber fees must be received by December 31st each year unless otherwise negotiated with the COE-Manager.

Appendix A: COE-Maritime Contact Information

1. COE-Maritime Management Team:

   - Navy Executive Agent for COE, Mr. Andrew Cox, PEO C4I TD, (858) 537-0526, andrew.cox@navy.mil
   - COE-M Manager/Technical Direction Agent, Mr. Wayne Duke, PEO C4I COE, (858) 537-0599, wayne.duke@navy.mil

2. COE-Maritime Customer Support Team:

   - Financial Assistant, Ms. Shelley Pino, (619) 572-2676, pinos@spawar.navy.mil
   - Technical Lead, Mr. Ted Brengel, , (858) 621-5458, tbrengel@spawar.navy.mil
   - Software Distribution POC, Ms. Cindy Taylor, (858) 553-7436, cindy@spawar.navy.mil
   - Test POC, Ms. Cathy Croswait, SSC SD D42, (619) 553-6057, croswait@spawar.navy/mil

3. Financial:

The COE-M Manager or Financial Asst. will direct all funding to one of the following addresses:

a. PEO C4I and Space
   4301 Pacific Highway
   San Diego, CA 92110-3127
   ATTN: Andrew Cox, PEO C4I

   (UIC for PEO C4I & Space is 3579A)

b. Commanding Officer
   Space and Naval Warfare Systems Center
   53560 Hull St.
   San Diego, CA 92152-5001
   ATTN: Judi Spears, Code 24201

   (UIC for Space and Naval Warfare System Center is N66001)

   If you need to discuss an issue with Ms. Spears directly, she can be reached by telephone at (619) 553-4031, or by email at jspears@spawar.navy.mil.

c. Commanding Officer
   Space and Naval Warfare Systems Center
   53560 Hull St.
   San Diego, CA 92152-5001
   ATTN: Cheryl Smith, Code 27304

   (UIC for Space and Naval Warfare System Center is N66001)

If you have a need to discuss an issue regarding funding sent to Ms. Smith, please contact Ms. Laura Hughes either by telephone at (619) 553-2754, or by email at lauralee@spawar.navy.mil.

In order to process your funding expeditiously, ALL funding documents should be faxed to the COE-M Manager at (619) 524-7414 (Attn: W. Duke) for payment processing and for execution of all SPAWAR funding. In addition, fax a copy of all SSC-SD Code 24201 funding documents to Judi Spears at (619) 553-4063 and SSC-SD Code 27301 funding documents to Laura Hughes at (619) 553-6365.

Appendix B: List of Applicable Web Sites

COE-Maritime Homepage – provides meeting reports, points of contact, schedules, upcoming events, access to distribution lists, STR/SCP entry and review, and download of COE documentation and software (software downloadable on by designated software recipients)
URL: https://coe.spawar.navy.mil

COE Homepage – central entry point for accessing COE information at DISA
URL: http://diicoe.disa.mil/coe/

COE XML Registry
URL: http://diides.ncr.disa.mil/xmlreg/index.cfm

SSC San Diego Software Support Activity (SSA) Homepage – provides configuration management information such as software media contents, software distribution, and also provides information on GCCS-M projects
URL: https://ssaweb1.spawar.navy.mil/

COE Newsgroups - these newsgroups are meant to help exchange information between the many people working COE, both directly on applications and DISA Personnel.
URL: http://diicoe.disa.mil/coe/newsgroups/

COE Configuration Management Page – segment registration, port/ID registration, CM numbers, delivery calendar, and GSPR Search
URL: https://dod-ead.mont.disa.mil/

COE Security Page
URL: http://diicoe.disa.mil/coe/coeeng/index2.html

COE Training
URL: http://diicoe.disa.mil/coe/training/

Appendix C: References

The following documents are of interest to the Maritime COE subscribers:

1. Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS), Version 4.1, 1 October 1998, Defense Information Systems Agency (DISA). This document describes the technical requirements for using the COE to build and integrate systems. It is available on the web at https://coe.spawar.navy.mil .

2. Common Operating Environment (COE) User Interface Specification, Version 4.1, 5 September, 2002, Defense Information Systems Agency (DISA). This document, sometimes called the COE Style Guide, defines the "look and feel" of the user interface for COE-based systems. The style guide provides specifications for applications using Motif and Windows GUIs, and Windows NT and Web-based applications. The document also contains the style requirements for compliance. It is available on the web at https://coe.spawar.navy.mil

3. Department of Defense (DoD) Joint Technical Architecture (JTA), Version 3.1, 31 March 2000, Joint technical Architecture Working Group. The JTA has been mandated by OSD directive for " . . . all emerging systems and system upgrades. The JTA applies to all C4I systems and the interfaces of other key assets (e.g., weapons systems, sensors, office automation systems, etc.) with C4I systems. The JTA also applies to C4I Advanced Concept Technology Demonstrations and other activities that lead directly to the fielding of operational C4I capabilities." The JTA stipulates compliance as part of its requirements. It also " . . . replaces the standards guidance in the Technical Architecture Framework for Information (TAFIM) currently cited in DoD Regulation 5000.2-R." This document is available on the web at https://coe.spawar.navy.mil.

4. COE Version Release Documentation, Defense Information Systems Agency (DISA). Various documents are provided with each software version release. These documents include user, support, and technical documentation on the Kernel, Infrastructure Services, Common Support Applications, and Software Development Services. The documents generally consist of Installation Procedures (IP), Software Version Description (SVD), Software User's Manual (SUM), System Administrator's Manual (SAM), Application programmer Interface (API) Reference Manual (APIRM) for each COE component. These documents are available by selecting the appropriate link on the web at https://dod-ead.mont.disa.mil/coe_docs/search.jsp

Appendix D: Key Roles and Responsibilities

PEO C4I TD – Navy Executive Agent for the COE

- Serve as the Navy Executive Agent for the overall management/coordination all COE matters for the Maritime services. This will include, but is not be limited to:
    - Provide overall technical and programmatic direction to the COE-M Manager for the execution of the COE in the maritime services.
    - Proactively identify and address maritime requirements/issues to the COE-M Manger and the DISA COE Chief Engineer.
    - Work with maritime programs to facilitate their migration to a COE based system
    - Establish COE Compliance Process for Maritime services
    - Provide an integrated COE testing capability

PEO C4I COE, COEM Manager and Technical Direction Agent (TDA)

- Manage/coordinate business/financial aspects of the COE-M program
    - Maintain up-to-date financial status of COE-M budget
    - Coordinate assignment and collection of COE fees
    - Coordinate establishment of tasking for COE-M infrastructure services
    - Coordinate with customers on funding issues.
- Provide COE technical direction/support
    - Serve Navy Rep at the COE Architectural Oversite Group (AOG)
    - Coordinate/provide COE technical support to for COE-M customers
    - Support COE related meetings including the SERG, AOG, and various IPTs/adhoc meetings with COE customers and coordinate COE-M Management Board meetings.
    - Coordinate Configuration Management of COE-M products with COE-M SSA
    - Coordinate maritime COE maintenance efforts
- Manage overall efforts of the Customer Support Team (CST)
    - Establish objectives/goals for CST and monitor progress toward achieving same
    - Facilitate solid communications and interaction between all members of the team
    - Coordinate regular CST meetings

COE Business Assistant

- Maintain COE financial spreadsheet
- Work financial issues with COE customers
- Coordinate the submission and processing of COE funding documents

Customer Support Team Technical Lead

- Supervises CST tasking at INRI
- Supports COE Manager/TDA in providing COE customers technical support
    - Support customer information queries regarding use of COE software and issues with same
    - Identifies customer issues and raises them to COE Manager/TDA to work with DISA/other parties as required.
- Coordinates support and maintenance of COE-M web site structure
- Manage COE software development/maintenance team efforts.

- Coordinate/document build requirements and software delivery schedules for COE-M products
  - Produce Software Development Plan addressing development/maintenance efforts and provide to PEO C4I.
  - Produce Functional Description Documents for all new development and provide to PEO C4I.
  - Work with COE Manager/TDA to identify Maritime issues with ICSF software and provide maintenance support to COE ICSF team to address same on an as approval/level of effort basis

Customer Support Engineers

- Provide technical assistance to developers on software and systems engineering matters
  - Provide telephone support in resolving software development/integration issues
  - Provide developers with sample code to facilitate their efforts on an as feasible basis
  - Provide on-site support, as authorized by the COE Manager/TDA, to resolve developer issues
- Provide COE Manager/TDA technical assistance in addressing process improvement efforts and resolving technical issues for subscriber programs
- Support COE related technical meetings as directed

Customer Software Requirements Coordinator

- Monitor and request changes to the COE-M Home Page to ensure customer software and documentation requirements are being met.
- Provide assistance to developers on software distribution issues.
- Notify SSA of new/changing customer information and requests software distributions

Configuration Manager

- Coordinates and manages all COE-M internal CM activities at SSC to ensure the timely execution and completion of assigned responsibilities within the Tasking Area.
- Resolves internal scheduling conflicts and resource overlap.
- Responds to complaints and issues as they relate to expected services from D4224 CM.
- Participates in the bi-monthly CMB and provides CM status slides for the briefing.
- Serves as the Navy Representative to the COE CM TWG.

Test and Evaluation (T&E) Lead

The T&E Lead is responsible to the Navy EA for maintaining a COE-M test facility and the execution of all required test events. The testing to be conducted is summarized as follows:

- From a Navy perspective, verify and document that delivered COE foundational products (primarily CCE/CME) exhibit the expected functionality, performance, and stability.
- Create a test bed environment for COE –M developers and DoD applications to participate in verifying system compatibility and interoperability.
- Evaluate software with a focus on system usability, equivalency, performance, scalability, compatibility, interoperability, maintainability, and security from the perspective of the end user of the COE in a C4I system environment.
- Stress the COE with applications and measure the system performance.
- Evaluate tiered replication capabilities in respect to the Navy requirements.

- Invite all Maritime customers to participate and submit their findings on performance via an established process.

On-Line Software Library Lead

- Maintains configuration control of all COE-M products.
    - Downloads software from the Asset Distribution System (DADS) for posting on the COE-M Library.
    - Ensures the software library has all approved software applications/segments, which have been approved for release.
    - Posts all software to the On-line library.
    - Removes superceded builds/applications
- Generates application media (tapes/CDs) in response to customer specific request for physical media.
- Maintains the Build List Worksheet.

Distribution Control Lead

- Coordinates distribution of all COE-M releases to approved subscribers.
    - Processes requests for software and documentation from approved subscribers, and ensures the COE-M test facility receives all software releases and updates.
- Ensures the subscriber/developer distribution database is updated to reflect new subscribers.
    - Reviews the developer distribution database periodically against the approved developer subscriber list to ensure accuracy and updates records as required.
- Responsible for formal acceptance of COE-M software and documentation from DISA.
    - Coordinates and inspects COE-M software and documentation to ensure compliance with established standards.
- Responds to queries on status of software shipments.
- Procures materials and media (tapes, CDs, labels, etc.) used for reproduction.

Appendix E: Maritime COE Management Board (CMB)

The CMB provides a formal mechanism for the Navy EA to provide subscribers with first hand management and technical information regarding the COE, software deliveries, COE issues/action items, and for soliciting input from the various Maritime programs which are using or plan to use the COE. Accordingly, this board establishes the forum for subscriber programs and their representatives to obtain the latest relevant information regarding the COE to voice requirements, share lessons learned, and to resolve issues concerning the implementation or migration to the COE. This will allow subscribers to communicate, debate technical issues, reach consensus, and provide a clear position as related to the development and evolution of the COE, which in turn can be forwarded to the SERG and/or the AOG as formal maritime requirements.

CMBs will be held every other month (on the third Wednesday when feasible) and will be conducted via VTC with primary VTC locations at SSC San Diego, CA and PRC, Crystal City, VA. Alternate/additional VTC sites can be accommodated with prior coordination with the Customer Support Team Lead. Minutes of the CMB proceedings, along with briefs, will be posted on the COE Maritime homepage within 5 working days after the CMB.

Appendix F: Maritime COE Configuration Control Board

1.0 Purpose

This charter provides guidance for the establishment and conduct of the Maritime COE Configuration Control Board (MCCB). This board is responsible for formulating Maritime requirements/technical positions and providing a consolidated input to the Systems Engineering Review Group (SERG), the Architectural Oversite Group, and the COE Engineering Office, as applicable. These requirements/inputs may be in the form of reviewed/processed software trouble reports (STRs/GSPRs) and software change requests (SCPs/GSPRs), validated/approved engineering change proposals (ECPs), and other technical and programmatic inputs as deemed appropriate.

2.0 Overview

The COE's development process, like that of any other program, is driven by three basic types of requirements - program schedules/milestones, the correction of problems with existing functionality, and the need for new functionality. Additionally, while fiscal realities often govern when something can be done, requirement delineation and the impacts of non-support of those requirements is the essential element in defining "what" is to be done. While Maritime programs may submit requirements directly to the Navy EA, the primary forums for the Maritime community to present and discuss their requirements are the COE Management Board (CMB) and this MCCB. Both boards provide a forum for subscriber programs to present their concerns, issues, requirements to the Navy EA and other maritime subscribers. By doing so, overlapping requirements, implementation issues, or other factors can potentially be identified that will allow better delineation of the "total maritime" requirement before it is forwarded to the appropriate COE body.

The MCCB has been established for two primary reasons. The first is to ensure that maritime subscriber programs understand the current status of outstanding Software Trouble Reports (STRs) and Software Change Proposals (SCPs). The second is to provide COE-M program office representatives a better understanding of the STR impacts or the urgency/dependency of SCPs to Maritime subscriber programs. Accordingly, this forum allows subscriber programs to present requirements and to have an input into the build process by discussing actual STR/SCPs that they either submitted or that have impact on their programs. As a result, the COE-M representatives will be better able to provide a consistent and technically sound input to DISA as to Maritime STR/SCP requirements for upcoming builds and patches releases.

3.0 MCCB and PCRB Relationship

The MCCB is analogous to the DISA COE Problem Control Review Board (PCRB) which meets on a weekly basis. This PCRB has the final say on COE component applications and problems/ enhancements against them. Each service has a representative supporting the PCRB and COEM's representative is the COEM SSA. During developmental/integration phases of new COE baselines, the vast majority of the problems/issues are found by either the DISA COE, COEM, or other service/agency test organizations, vice the developer/user community. Due to this fact and the volume of issue, it has proven more efficient to not hold MCCB during this phase and to concentrate the efforts on coordination at the weekly PCRBs. During this period, it individual

developers have specific issues/inputs, they should forward same to the COE Manager/TDA for input to the PCRB. Additionally, results of the PCRBs are input into the history field of each SCR. Once a firm, stable COE baseline is established and we find more STRs originating from COEM developers/users, MCCBs will be scheduled on a regular basis to discuss/review new/open STRs.

Due to the time, effort required to support both MCCBs and weekly PCRBs, if participation in the MCCB is not sufficient to warrant holding the meeting, MCCBs will be discontinued and the process used during the developmental phase will be re-established.

4.0 MCCB Responsibilities

Review all newly submitted STRs/SCPs to ensure that all require information is provided, that they are technically accurate and clearly understandable, that prioritization is appropriate, and that any relevant impact information or applicable comments are documented. On a practical basis, normally only priority-1, 2, and depending on volume, priority-3 STRs and priority 1 and 2 SCPs will be covered during actual telcon. Lower priority STRs/SCRs not covered during actual MCCB will be reviewed during an Admin MCCB by the COEM Manager/TDA, COEM test engineer, and an SSA rep with the results entered into the CM database.

Submit results of MCCB STR/SCP processing to COE-M SSA for database update and for submission of STRs/SCPs to the DISA GSPR database on COE components.

Review newly submitted ECPs for technical accuracy and provide forum for originating program to brief their ECP in order to identify overlapping requirements, implementation issues, potential co-sponsorship, or other factors can potentially impact the ECP. Upon completion of review/ processing of ECPs, make recommendation for approval or disapproval to the Navy EA.

Submit results of MCCB ECP processing to COE-M SSA for database update and to the Navy EA for final approval, then forward to appropriate TWG and/or DISA COE Engineering Office, as appropriate.

Based on MCCB discussions and program inputs, prepare a consolidated and prioritized Maritime COE requirements list for both STRs and SCPs/ECPs.

Coordinate with the COE-M SSA to ensure that non-maritime STRs originated by other COE communities are accessible for review and comment by the MCCB.

Provide a forum to validate/consolidate inputs from AOG action items, COE “data calls”, and/or other technical issues prior to submittal to DISA.

Establish a MCCB list server for forwarding of MCCB information/agendas.

Maintain record of their actions, status of issues, and status of requirements.

The Chairman shall work with the COE-M SSA to ensure all STR/SCP/ECP is accurately maintained and available to the subscriber community and MCCB.

The COEM Manager/TDA shall coordinate with DISA COE Engineering facilitate incorporation of the maritime requirements into the COE builds/patches.

4.0 Meetings

MCCB will be convened on normally on a twice a month basis, though this may vary from weekly to once a month dependent on the volume of STRs/SCPs. They will be conducted via "dial-in conference calls" and will focus on the review/processing of newly submitted STRs/SCPs. Previously reviewed STRs/SCPs, ECPs, and other technical issues may be discussed on a time-available basis). The intent will be to keep MCCBs to a maximum of one hour.

At the regularly scheduled COE-M Management Board (CMBs), MCCB STR/SCP status/summary information, briefings of proposed maritime ECPs, and proposed consolidated maritime priorities for future COE builds/patches will be presented. These meetings will focus on STR/SCP/ECP status and summary information, introduction and validation of maritime ECPs, and on obtaining consolidate maritime priorities for future COE builds/patches (will not normally actually review/process new STRs/SCPs.

Notification of and agendas for the MCCBs will be automatically sent to all individuals registered on the MCCB list server and will be posted on the COE Maritime website.

5.0 Representation/Participation

The MCCB shall be chaired by the COE Manager/TDA or his designated alternate. All Maritime COE subscriber programs are strongly encouraged to participate as members of the MCCBs. While each program should designate a representative to formally represent them at the VTC'ed CMB/MCCBs, participation at telcon MCCBs is open to all interested maritime subscriber affiliated personnel. To avoid confusion and excessive conference expenses, it is requested that the number of representatives of each program be kept to a minimum and that they are knowledgeable regarding the use and functionality of the COE and their system/application.

Appendix G: COE CRCB, AOG, and SERG

There are three DISA level forums where Maritime requirements can be addressed. These forums are the COE Configuration Review and Control Board (CRCB), the Architecture Oversight Group (AOG), and the System Engineering Review Group (SERG).

The CRCB is a Flag level forum for setting objectives and priorities for the COE as well as overseeing processes used for COE development and deployment. The CRCB will approve recommended changes to the COE, approve build plans, and make recommendations for the expansion of the software and hardware base for COE. It will approve all retirements of published Application Programmer Interfaces (APIs).

The AOG is chaired by the DISA COE Chief Engineer and consists of a representative members from each Services/Agency using the COE. This body has the responsibility for formulation of the top level architectural guidance for the COE and to ensure that the requirements of the Services/Agencies addressed.

The SERG is co-chaired by the DISA COE Chief Engineer and the DISA NCES Chief Engineer and consists of a representative from each of the services/agencies. This body has the responsibility to support the COE/NCES Program Office in resolution of technical issues, planning for technology insertion involving , providing input on the impacts of such items on their services/agencies. This group will meet on a monthly basis and where required, will stand-up sub-groups to work specific technical issues.

Appendix H: COE-M Subscriber Support Services

I. **Basic Services:** The COE Navy EA will, under the basic fee structure, provide the following services:

- COE Program Management
- COE Integration and Maintenance Team
- Subscriber Program technical support
  - ◊ Maintain a Customer Support Team (CST)
  - ◊ Assist programs with COE migration strategies/addressing programmatic issues
  - ◊ Provide system/software engineering support to system developers to resolve technical issues
- Configuration management
  - ◊ Conduct Maritime Configuration Control Board Meetings
  - ◊ Status accounting
  - ◊ COTS enterprise and non-enterprise license distribution and tracking
- COE component segment Life Cycle Management
- GFI/GFE Control and Planning
- Software and documentation (soft copy only) distribution
  - ◊ Distribution on appropriate computer media automatically with new releases and upon request
  - ◊ Distribution via website
- Coordination, Planning and Representation on Joint CCB for Maritime requirements
  - ◊ Working Group Support
  - ◊ Integrated Product Team (IPT) Support
- Standards Review
- Hardware requirements review and status

Extended Services: Additional services, beyond those provided under this plan may be available through the Maritime Executive Agent at additional cost to the requesting program. These services may include (but are not limited to):

- Additional system engineering support beyond that support above.
- On-site software engineering support to assist developers with understanding and using the COE's development environment
- Software development of program segments
- COE enhancements to support program requirements (must be in conjunction with COE ECP process)

In general these services will be provided by one of the contractors supporting the EA and will be provided on a first-come-first-serve basis using available personnel resources. Before requesting these services, program personnel should discuss their needs with a member of the Customer Product Support Team and draw up a support requirements list to be addressed by the extended support. Finally, a request for the extended services required should be submitted to the EA and BFM.

Appendix I: COE Compliance

This appendix provides an overview of Compliance and then on the Compliance validation and waiver process in the maritime community.

1. Compliance Overview: The COE (Common Operating Environment) concept is best described as an architecture that is fully compliant with the DoD Technical Architecture for Information Management (TAFIM). The TAFIM Volume 3, an approach for building interoperable systems, is a reference implementation containing a collection of reusable software components, a software infrastructure for supporting mission-area applications, and a set of guidelines, standards, and specifications.

COE compliance is closely associated with interoperability, and for this reason systems are increasingly being measured by the degree to which they meet compliance requirements. OSD has issued a directive that all new C4I systems and other systems, which interface to C4I systems, shall be in compliance with the Joint Technical Architecture (JTA). The JTA in turn mandates use of the COE. While the JTA currently only addresses information and C^4I systems, it is being expanded in scope to address weapons systems as well.

The COE is primarily concerned with the executable environment of a system and is specifically designed to be programming-language neutral. The COE is a plug and play open architecture. The current reference implementation is designed around a client/server model. The COE is not a system; it is a foundation for building an open system. Functionality is easily added to or removed from the target system in small manageable units called segments. Structuring the software into segments is a powerful concept that allows considerable flexibility in configuring a system to meet specific mission needs or to minimize hardware requirements for an operational site.

Backward compatibility is a fundamental tenet of the COE and significant effort is expended to preserve legacy investments. Systems that migrate to the COE now are protected by backward compatibility as future COE versions are released. Upgrading from one COE version to the next is generally no more difficult than upgrading from one COTS product version to the next.

The COE defines four areas in which compliance is measured, shown in the figure below, called compliance *categories*. Within a specific category, a segment is assigned an integer value, called the compliance *level*, which is a measure of the degree to which a segment is compliant within that category. The COE takes this approach because it is especially useful in developing migration strategies for legacy systems. Compliance categories indicate the broad area in which a segment must be improved while compliance levels express the degree to which the segment meets COE objectives within that category.

The four compliance categories are:

> **Category 1: Runtime Environment.** This category measures how well the proposed software fits within the COE executing environment, and the degree to which the software reuses COE components. It is an assessment of whether or not the software will "run" when loaded on a COE platform, and whether or not it will interfere with other segments. This category is closely related to, and is a way of measuring, interoperability.

Category 2: Style Guide. This category measures how well the proposed software operates from a "look and feel" perspective. It is an assessment of how consistent the overall system will appear to the end user. It is important that the resulting COE-based system appear seamless and consistent to minimize training and maintenance costs.

Category 3: Architectural Compatibility. This category measures how well the proposed software fits within the COE architecture (client/server architecture, DCE infrastructure, CDE desktop, etc.). It is an assessment of the software's potential longevity as the COE evolves. It does *not* imply that all software must be based on client/server or Remote Procedure Call (RPC) techniques. It simply means that a reasonable design choice has been made given that the specific architectural characteristics of the COE reference implementation.

Category 4: Software Quality. This category measures traditional software metrics (lines of code, McCabe complexity metric, etc.). It is an assessment of program risk and software maturity.

Runtime Environment	Style Guide	Architectural Compatibility	Software Quality
0 → j	0 → k	0 → n	0 → m

The principles and techniques described in the remainder of this paper apply to each of the compliance categories. However, only the compliance levels for the Runtime Environment Category will be discussed any further. The COE defines eight progressively deeper levels of integration for the Runtime Environment Category. These levels are directly tied to the degree of interoperability. Note that levels 1-3 are interfacing with the COE, not true integration. True integration begins at level 4, though the minimal acceptable COE compliance is level 5. This level basically ensures that applications can peacefully coexist in a given system and operate using the basic kernel infrastructure features.

Level 1: Standards Compliance Level. A superficial level in which the proposed capabilities share only a common set of COTS standards. Sharing of data is undisciplined and minimal software reuse exists beyond the COTS. Level 1 may, but is not guaranteed to, allow simultaneous execution of the two systems.

Level 2: Network Compliance Level. Two capabilities coexist on the same LAN but on different CPU's. Limited data sharing is possible. If common user interface standards are used, applications on the LAN may have a common appearance to the user.

Level 3: Platform Compliance Level. Environmental conflicts have been resolved so that two applications may reside on the same LAN, share data, and coexist on the same platform. The COE kernel, or its equivalent, must reside on the platform. Segmenting may not have been performed,

but some COE components may be reused. Applications do not use COE services (except for kernel services if the COE kernel is loaded) and are not necessarily interoperable.

Level 4: Bootstrap Compliance Level. All applications are in segment format and share the COE kernel. Segment formatting allows automatic checking for certain types of application conflicts. Use of COE services is not achieved and users may require separate login accounts to switch between applications.

Level 5: Minimal Compliance Level. All segments share the same COE kernel and functionality is available via the Executive Manager. Boot, background, session, and local processes are specified through the appropriate segment descriptors. Segments adhere to the basic look and feel of the native GUI, as defined in the User Interface Specification. Segments are registered and available through the online library. Applications appear integrated to the user, but there may be duplication of functionality and full interoperability is not guaranteed. Segments may be successfully installed and removed through the COE installation tools. Database segments are identified as unique or sharable according to their potential for sharing.

Level 6: Intermediate Compliance Level. Segments utilize existing account groups, and reuse one or more COE-component segments. Minor documented differences may exist between the User Interface Specification and the segment GUI implementation. Use of non-standard Query Language (SQL) in database segments is documented and, where applicable, packaged in a separate database segment.

Level 7: Interoperable Compliance Level. Segments reuse COE–component segments to ensure interoperability. These include COE-provided communications interfaces, message parsers, database segments, track data elements, and logistics services. All access is through published APIs with documented use of few, if any, private APIs. Segments do not duplicate any functionality contained in COE-component segments. The data objects contained within a database segment are standardized according to DoD 8320 guidance.

Level 8: Full Compliance Level. Proposed new functionality is completely integrated into the system (e.g., makes maximum possible use of COE services) and is available via the Executive Manager. The segment is fully compliant with the User Interface Specification and uses only published public APIs. The segment does not duplicate any functionality contained elsewhere in the system, whether as part of the COE or as part of another mission application or database segment.

2. Compliance Validation and Waivers:

Overall Guidance: An ASD C3I letter of 23 May 1997 mandated COE level-6 as the minimum level of compliance, with the goal of achieving level-7 (though this has been relaxed to level-5 for programs "forging the way" to field initial COE based systems). As previously stated, level 5 compliance basically ensures that applications can peacefully coexist in a given system, while Level 7 compliance requires common utilization of core services (common support applications) such as Joint mapping Toolkit (JMTK) and Track Management System (TMS). Additionally, for numerous programs/systems, COE compliance has been stipulated in the ORD. Level 6 compliance allows some duplication of COE core services/common support applications. Appendix B of the I&RTS

provides the COE Compliance Checklist which is utilized to validate the compliance level of COE based segments. To be complaint to a given compliance level, a segment must meet all checklist requirements of that level and all preceding levels (e.g., even if a segment meets all level 5 and 6 requirements, if it does not comply with a level 4 requirement, the highest compliance level for that segment is level 3). The I&RTS does, however, allow a waiver process which takes into consideration issues such as unique requirements that may be in conflict with a particular checklist item or issues brought about by deficiency in the COE. Waivers are not granted items where a program disagrees with the requirement or feels it is simply not applicable to their application.

The I&RTS gives the DISA COE Chief Engineer the authority to grant COE compliance waivers, who in turn has passed that waiver authority to each service for service unique segments (those not submitted to DISA for use by the joint community). For the maritime services (Navy and USCG), the Navy Executive Agent is responsibly for establishment and oversight of a cohesive waiver process. Each service/agency has established compliance policies that range from a centralized process with all waivers being approved by a single waiver authority to a more decentralized policy that puts the focus/responsibility on the Program Manager of the end system. Due to the diversity of the COE-M subscriber programs and their sponsorship from various systems command, COE-M has chosen the latter approach as is described in the following section. Regardless of the process, it is essential that the Program Sponsors, Managers, and certifying agency (e.g., COMOPTEVFOR) consider compliance issues/waivers early in the development cycle to establish a success-oriented approach to ensure that all potential compliance issues are either resolved or are waiverable.

COE Maritime Waiver Process: The decentralized compliance policy established for COE-M places the authority and responsibility to administer waivers in the hands of the Program Manager for the individual system. It is the Program Manager's responsibility to ensure that the system he controls meets all established requirements and COE compliance is consider as one of those requirements. Each program should establish a process to validate the compliance level of all COE segments and recommend either approval or disapproval of submitted waivers. This process can included a formal test and validation activity or place the burden of validating compliance on the software developer. Most programs will chose the latter, but regardless, the segment developers should be required to evaluate each of their applications/segments against the requirements of Appendix B to the I&RTS and provide the a completed Appendix B to the program indicating that each items is either satisfied, not applicable, or not satisfied. For items, not satisfied, they should either provide a formal waiver with justification for same or identify how they are going to address the issues for items at or below the goal compliance level. Note that the justification can be technical or programmatic (e.g., significant additional cost do not warrant addressing the item; using COTS product; schedule does not allow time to address and will address on next delivery; etc.).

To aid the program with the review of waivers, the COE-M office will, if requested, review waivers for a program and give recommendations based on our understanding of the I&RTS requirements and history of the process. COE-M will recommend disapproval for any waiver that appears due to circumvent the I&RTS, where a program disagrees with the requirement or feels it is simply not applicable to their application, or when a developer/program significantly duplicates COE software capability. With that said, COE-M has historically recommended over 80% of requested waivers when they are adequately justified and do not impact interoperability with other application. The Program Manager is free to use the recommendations or rely upon his own judgment or that of his

technical staff. In any case, whether the waiver request be for technical or programmatic reasons, the key issue that must be considered in granting the waiver is its potential impact on interoperability with other applications loaded own the workstation or LAN. Note, that if asked by the certifying activity (e.g., COMOPTEVFOR) to review waivers granted by a program, the COE-M office would do so and provide the same response as initially provided to the program. In the case of differences of opinion, the suitability of the waivers will then be subject to the certifier's discretion.

The key to a successful waiver process is pre-planning and establishing a validation/waiver process up-front, ensuring that developers understand that compliance requirements are not "optional" but required, and working with the COE-M office as required for technical support and/or review of the process or waivers.

Appendix J: COE-M Software Change Request (SCR) Process, Segment Registration, and Software Distribution

Software Change Request (SCR) Process

A Software Trouble Report (STR) is used to report software deficiencies or problems with software failing to meet baseline requirements (specified in the applicable requirements document). A Software Change Proposal (SCP) is used to submit recommended enhancements to currently supported requirements. STRs and SCPs are collectively referred to as Software Change Requests (SCRs). Forms for submitting SCRs against COE are available on the COE-Maritime Website (https://diicoe.spawar.navy.mil). The submitted SCRs are maintained in the Configuration Management Accounting System (CMAS) maintained at the COE-M Software Support Activity (SSA).

The Maritime COE Configuration Control Board (MCCB) will review all COE-M SCRs, consider appropriate technical issues and recommend specific actions. The MCCB may adjust SCR prioritization based on compliance with IEEE 12207 specification. Any changes to the original SCR will be documented in the SCR history. This forum allows subscriber programs to present requirements and to have an input into the build process by discussing SCRs that may have an impact on individual programs. The collective input will then be sent to DISA as the COE-M requirements for upcoming builds and interim software releases. STRs are reviewed by the DISA Program Change Review Board (PCRB) and assigned to future builds in accordance with priorities. SCPs are reviewed by the SERG or appropriate sub-group, who provide a recommendation on implementation priority and build assignment. The MCCB process is further discussed in Appendix F.

Engineering Change Proposals

While Software Trouble Reports and Software Change Proposals address deficiencies in or changes to established requirements, an Engineering Change Proposal (ECP) documents new requirements or significant modifications to established requirements. Once a program identifies a requirement that they consider applicable to the COE infrastructure/services, they should document the same using the ECP format provided Appendix M of this plan. Besides documenting the details of the requirements and substantiating the need for same, the ECP provides additional information as to ILS impacts, potential impact on computer resources (e.g., RAM, CPU, memory), schedule, and estimated cost, etc.

Draft ECP's are submitted to the Maritime COE Office and reviewed by the technical staff and any questions/issues directed to the originator. Once the ECP review process is completed, the originating program will be given the opportunity to discuss the ECP at MCCB's and to brief the ECP at a DMB in order to identify overlapping requirements, implementation issues, potential co-sponsorship, or other factors could potentially impact the ECP. This ECP presentation/briefing is not required and if the Navy EA considers the ECP technical valid and the program is prepared to fund the ECP, the ECP can be forwarded to DISA for processing and implementation as will those that are briefed at MCCB's (ECP's to Maritime Extensions to the COE will be implemented by the Navy EA).

Next to the validity and priority of the requirement, one of the key factors affecting implementation of ECP's, is the funding of same. Dependent on the nature of the ECP, the cost for incorporation may be covered by DISA, by the Maritime COE Program Office, or may fall on the program(s) submitting the request. While ECP's, especially those of more general applicability, have greater likelihood of DISA covering implementation costs, the overall priority of requirements from the services and agencies, may delay the implementation beyond the timeframe needed by the requestor. In these cases, the program(s) requesting the ECP can cover the cost and accelerate the implementation if desired. For ECP's which are more uniquely tied to a given program, the submitting program(s) will be responsible for funding the implementation and can coordinate the funding through the Maritime COE Office.

All submitted ECP's will be tracked in the CMAS database from submittal through implementation or withdrawal/closure.

Segment Registration

Per I&RTS policy, all programs must register segment-related information as early as possible in the development cycle. Segments are registered with DISA at https://dod-ead.mont.disa.mil/help/register_segment_help.jsp. This page details instructions for registering prefixes, software segments, TCP/UDP Sockets, User IDs (UID) and, Group IDs (GID). At a minimum, the segment prefix should be reserved to avoid conflicts with other joint software developers. A software segment is registered prior to delivery to DISA. TCP/UCP Sockets, UIDs and GIDs are registered for segments that require them.

Software Distribution

COE Software is distributed only to program designated software recipients. Each subscriber program designates one or more designated software recipient(s). As new builds are released, the designated software recipients will automatically receive a package via FedEx. The package will contain one copy of the software and documentation (requests for additional copies should be sent to the COE Manager/TDA or Customer Support Team Lead). These builds will also be available for download by the designated software recipient from the Maritime COE Maritime Home Page (https:// coe.spawar.navy.mil). Interim software and documentation releases will also be available for download and will only be shipped upon request. As software and documentation become available, a Maritime COEgram will be sent via the COE List Servers. Instructions for subscribing to the List Servers are available on the COE Maritime Home Page. Software requests and any changes to program designated software recipient information should be directed to the COE-M Software Distribution POC (see Appendix A).

Appendix K: COE License Requirements and Management

The Maritime Defense Information Infrastructure Common Operating Environment (COE-M) program contains software segments comprised of Commercial Off-the-Shelf Software (COTS). Currently COE subscriber fees do not include licenses for these COTS segments. To legally use the COE COTS segments, subscribers must have and maintain a license from the software vendor.

Some COTS segments are licensed under a Department of Defense (DoD) Enterprise License agreement (eg. Netscape), while others are public domain (no license required), these segments do not require licensing by the subscriber.

In some cases a COE-M program sponsor MAY obtain licenses for their subscribers, allocating them on an individual basis. Subscribers not allocated a license by their program sponsor must demonstrate proof of license prior to distribution of the software by the COE-M Software Support Agency (SSA). The subscriber's proof of license should normally be in the form of a valid license number. For those cases where the vendor did not provide a unique license number with product, or a generic number is provided for licenses purchased in bulk, a copy of the packing slip or signed purchase order/invoice to validate proof of purchase. In either case, the SSA will verify with the vendor.

The COE-M SSA performs tracking and management of COTS licenses. Through coordination with the COE-M Program and Project offices, the SSA is provided a list of those organizations having paid subscriber fees and, when applicable, to whom licenses are extended. In this manner the SSA is able to identify those subscribers eligible to download software segments, and to whom licensing is granted through the project sponsor.

Appendix L: Maritime Extensions

The Maritime Extensions are the components that were unique to the maritime community and removed from the original JMCIS COE when it became the COE. As discussed in section 2 of this plan, these removed maritime components/extensions are now maintained by the COE-M and are added to the baseline COE before distribution to the maritime subscribers as COE-M. In COE 3.X, these "extensions" include MAREXT, COMEXT, Common Printers, and JMCIS Dev (provides libraries to utilize the old Alert services that are still in the COE but not supported by DISA). In COE 4.X, the maritime extensions are only C4I Common Extension and C4I Maritime Extensions, (CCE and CME) and their software development kits (SDK's). CME contains primarily Navy specific interfaces and a few Navy specific TDAs, while CCE provides some more generic interfaces and additional TDAs/applications that can be used in a Joint C4I environment. The SDK's provide API's associated to specific contained functionality. It is important to note that these additional components in no way alter the baseline COE or impact an applications/segment's ability to function on straight COE based system (it will not, however, have access to the additionally provided functionality).

A summary of the contents of the Maritime Extensions to the COE is provided below. More detail can be obtained in the User's Guides.

C4I Maritime Extensions		C4I Common Extensions	CCE/CME SDK
Tactical Decision Aids	**Interfaces**	**Tactical Decision Aids**	**API's**
NTDS Symbology	AC DS Blk-0	GEOSIT	Pimtracks,
Limit Lines of Approach	SRN19	PIMTRACK (routes)	Screen Kilo,
4Whiskey	GPS (SRN25)		Four Whiskey,
Screen Kilo	GFCP		& NTDS
Track History Analysis	SPA25G		
Quick CPA	CVNS		
Quick Intercept	TAMPS	**Interfaces**	
Search and Rescue	NAV	NMEA 0183	
2-Track Analysis	NAVSSI	OTCIXS/TADIXS	
Cap Engagement	WSN5	Link-14	
Status Boards	WRN6		
Time-Late Statistics			
Navy Sites			
Crossfix			
Bearing Overlay			
Nav Update Rate			
Briefing Slides (UNIX)			
NTDS Symbology			

Appendix M: Engineering Change Proposal (ECP) Format

Provided below is the format for preparation of COE-M ECPs. Assistance in preparation of the ECPs can be obtained from the COE-M Customer Support Team.

ENGINEERING CHANGE PROPOSAL (format)

DATE
PROGRAM (program sponsoring change)
CLASS (I or II per MILSTD definition)
PROCESSING PRIORITY (E - emergency, U- urgent, R - routine)
ECP NO (assigned by COE-M SSA)
TYPE (preliminary or formal)
REV (basic or revision number)
TITLE (short descriptive title)
SPECIFICATIONS (attach preliminary SRS requirements table update)
DESCRIPTION CHANGE (provide complete details of the ECP)
NEED FOR CHANGE (reference NCRs & short titles):
EFFECTIVITY (COE release numbers)
ESTIMATED COSTS/ FUNDING (cost should include and be broken out for COE software development, any SSA/Integration support required, and anylife cycle cost that may apply)
DEVELOPMENTAL REQUIREMENTS (GFE/GRI requirements, COE requirements, other)
ILS IMPACTS (hardware, training, etc)
OTHER CONSIDERATIONS (e.g. certification, RAM/CPU usage, changes to the COE core)
SCHEDULE

The below implemented ECP is provide as an example.

DATE:	Oct 24, 1996
PROGRAM:	PMW-171, JMCIS Afloat
CLASS:	I
PROCESSING PRIORITY:	URGENT
ECP NO:	0024
TYPE:	PRELIMINARY
REV:	COE 3.0.2.X/3.X
TITLE:	ATOX II Enhancements

SPECIFICATIONS: Implement ATOX II Enhancements as specified in the ATOX II FDD.

DESCPRIPTION CHANGE:

This ECP addresses COE Software Change Proposal DU00621 which addresses the expansion of the ATOX functionality currently available in the COE to provide the user increased capability to graphically display and handle selected ATO and ACO information. The primary areas addressed are:

- automated geographic association of targets or mission locations and tracks assigned to those targets or locations.
- geographic display of ACO information (ingress/egress points, rendezvous points, air corridors and other Airspace Control Means (ACMs))
- access to the majority of the ATOX II functionality from any computer system on the tactical LAN using a commercial standard browser application via connection to the COE Hypertext Transfer Protocol (http) server.
- improved access to CDBS information on ATO targets.
- export of data to COTS applications for display of ATO and ACO data in chronological, tabular and textual formats.

NEED FOR CHANGE:

Joint air operations require increasing awareness and use of Air Tasking Order (ATO) and Airspace Control Order (ACO) information. GCCS and JMCIS systems are currently capable of receiving ATOs directly from CTAPS or via other means, processing the information, and formatting it in such a manner that it may be forwarded to other JMCIS/ GCCS sites. Additionally, ATO mission data can be displayed on the tactical display and manual associations between system tracks and the ATO missions can be made. The ATOX II/Air Task enhancements supported by this ECP provide needed automatic associations between targets and tracks prosecuting a given ATO target, supports ACO processing/display and the export of ATO/ACO data to standard PC COTS utilities, and provides improved interface to CDBS information

These enhancements address the warfighter's requirement for improved tactical situational awareness during the planning and execution of ATO missions. The enhanced display of ATO and ACO information will allow users to more easily visualize tasked air operations and associate a given ATO mission with target, track or airspace control objects on the tactical display. These enhancements will also be accessible across the tactical intranet from other computer systems using commercial standard browsers and thus extend the functionality to the PC/NT workstations.

EFFECTIVITY: 3.0.2.X/3.X

ESTIMATED COSTS/FUNDING: $420,000.

Current $350,000 funding level from PMW-171 supports the implementation of the ATOX II capability in the HP 3.0.2.4/5 environment (with JMTK/CR1) to support Naval COE OT requirements only. It does not support porting to the 3.0.2.X Solaris environment nor the migration to COE 3.X (with JMTK/CR2). Estimate cost for porting to a 3.0.2.X Solaris environment is $20,000 and for migration to the 3.X HP and Solaris environments is $50,000.

DEVELOPMENT REQUIREMENTS:

1. No additional developmental hardware resources are required.
2. Estimated software engineer requirements are 5 engineers for 5-6 months for HP 3.0.2.X implementation.
3. An additional 1.5 man-months is required for a 3.0.2.X Solaris port and 4 man-months for the COE 3.X migration.

ILS IMPACTS:

1. The primary ILS impact will be the necessity to ensure changes of the USMTF message specifications for ACO's are incorporated as changes occurs.

OTHER CONSIDERATIONS:

1. The processing of the ACO message will require USMTF certification.
2. This ECP must be submitted to the COE CCB to obtain approval for integration into the COE Core software. This capability can be maintain as a Naval COE ATOX II Core Segment if desired and not migrated to the core.
3. This ECP will require changes to two current COE modules/files (CommDec and Ato) and will add several new modules/files to support the ACO processing/display and other introduced functionality.
4. The overall effect on RAM and CPU usage is estimated to be insignificant.

SCHEDULE: The ATOX II enhancements will initially be provided as a Naval COE ATOX II Patch Segment to the COE version 3.0.2.4/5. This will be accomplished in a three phased implementation process:

1. Phase I will provide basic ACO processing/display and support the export of ATO/ACO data and will be delivered in to NRaD for testing on 6 Mar 97.
2. Phase II will complete the incorporation of all FDD requirements to the maximum extent possible (as limited by funding and delivery schedule) and shall be delivered to NRaD approximately in May 97 (specific date will depend on certification testing date).
3. Phase III will be address correction of STR's identified in NRaD and/or certification testing with specific schedule tbd.

After successful completion of functionality and certification testing, the ATOX II capability can be integrated into the baseline 3.0.2.X software in the next upgrade/patch (date tbd) and into the 3.X COE baseline (version/date tbd) pending approval by the CCB and identification of required funding.

Appendix N: Acronyms and Definitions

This Appendix Eefines the acronyms and terms which are used throughout the FY00 Plan for Management and Support of COE for Maritime Customers and its appendices.

M.1 Acronyms

ACDS	Advanced Combat Direction System
ACM	Airspace Control Means
ACO	Airspace Control Order
ASD	Assistant Secretary of Defense
API	Application Program Interface
APIRM	Application Program Interface Reference Manual
APPs	Applications
AOG	Architecture Oversight Group
ATO	Air Tasking Order
ATOX	Air Tasking Order Transmit
BFM	Business Financial manager
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
CCB	Configuration Control Board
CDBS	Central Database Server
CDE	Common Desktop Environment
CFCSE-IC	Center for Computer Systems Engineering Information Clearinghouse
CI	Configuration Item
CINC	Commander-in-Chief
CM	Configuration Management
COB	Close of Business
COE	Common Operating Environment
COMEXT	Common Extensions
COMOPTEVFOR	Commander Operational Test and Evaluation Force
COTF	Commander Task Force see Bruce
COTS	Commercial Off-the-Shelf Software
CPA	Closest Point of Approach
CPU	Computer Processing Unit
CR	Cartographer
CST	Customer Support Team
CTAPS	Contingency Theater Automatic Planning System
CY	Calendar Year
DB	Data Base
DCE	Distributed Computing Environment
DII	Defense Information Infrastructure
COE M	COE Maritime
DISA	Defense Information System Agency
DMB	COE M Management Board
DNS	Domain Name Server
DoD	Department of Defense
DOL	COE On-line Library
DT	Developmental Test
EA	Executive Agent

ECP	Engineering Change Proposal
FDD	Functional Description Document
FMS	Foreign Military Sales
FRB	Foreign Releasibility Board
FY	Fiscal Year
GCCS	Global Command and Control System
GCCS-M	Global Command and Control System - Maritime
GCSS	Global Combat Support System
GFCPLAN	Generic Front End Communications Processor Local Area Network
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GRI	Government Requested Information
GUI	Graphic User Interface
HP	Hewlett Packard
HPUX	Hewlett Packard UNIX
HQ	Headquarters
HTML	Hyper-Text Markup Language
HULTEC	Hull-to-Emitter Correlation
I&RTS	Integration and Runtime Specification
I/F	Interface
ILS	Integrated Logistics Support
IP	Installation Procedures
IPT	Integrated Product Team
JIEO	Joint Interoperability and Engineering Office
JMCIS	Joint Maritime Command Information System
JMTK	Joint Mapping Tool Kit
JPL	Jet Propulsion Laboratory
JTA	Joint Technical Architecture
K	Thousand
LAN	Local Area Network
LCCB	Local Configuration Control Board
LORAN C	Long Range Navigation C
M	Million
MARCORSYSCOM	Marine Corps Systems Command
MAREXT	Maritime Extensions
MCCB	Maritime COE Configuration Control Board
MCG&I	Mapping, Cartographer, Graphic, and Imagery
MCTSSA	Marine Corps Tactical System Support Activity
MILSTD	Military Standard
MIPR	Military Interdepartmental Purchase Request
MIT	Massachusetts Institute of Technology
NAVMASSO	Navy Maintenance System Support Office
NAVSSI	Navigation Sensor System Interface
NIS	Network Information Service
NLT	No Later Than
NRaD	Naval Research and Development
NSWC	Naval Surface Warfare/Weapons Center
NT	New Technology

NUWC	Naval Undersea Weapons Center
O&M	Operations and Maintenance
OPN	Other Procurement, Navy
ORD	Operational Requirements Document
OS	Operating System
OSD	Office of the Secretary of Defense
OT	Operational Test
OTCIXS	Officer In Tactical Command Information Exchange Subsystem
OVLY	Overlay
PC	Personal Computer
PD	Program Directive
PDF	Portable Document Format
PMW	Program Manager, Warfare
PRC	Planning Research Corporation
QA	Quality Assurance
R&D	Research and Development
RAM	Random Access Memory
RCP	Request for Contractural Procurement
RPC	Remote Procedure Call
SAM	System Administrator's Manual
SAR	Search and Rescue
SCCB	Subscriber Configuration Control Board
SCP	Software Change Proposal
SCR	Software Change Request
SDE	Software Development Environment
SHADE	Shared Data Environment
SIWG	System Integration Working Group
SPAWAR	Space and Naval Warfare Systems Command
SQL	Standard Query language
SRS	Software Requirements Specification
SSA	Software Support Activity
SSAS	Software Support Activity System
SSC	SPAWAR System Center
SSC-SD	SPAWAR System Center – San Diego
STR	Software Trouble Report
SUM	Software User's Manual
SVD	Software Version Description
SW	Software
SYSCOM	Systems Command
TAFIM	Technical Architecture for Information Management
TAMPS	Tactical Automated Mission Planning System
TDA	Technical Design Agent; Tactical Decision Aid
TDBM	Tactical Data Base Management
TMS	Track Management System
TWG	Technical Working Group
URL	Uniform Resource Locator
USAF	United States Air Force
USCG	United States Coast Guard
USMC	United States Marine Corps
USMTF	United States Message Text Format

USN	United States Navy
VTC	Video Teleconference
WR/WX	Work Requests
www	World-Wide-Web

M.2 Definitions

Application Programmer Interface (API) — APIs provide system services and data base access through published interfaces. APIs are approved by DISA, which guarantees forward compatibility through successive builds unless changes are formally announced. API additions, deletions, and changes must be approved by DISA.

Approved Software — Software that has been tested as compatible with the COE. In this context, approved software implies only that the software has been tested and confirmed to work within the COE. It does not imply that the software has been approved or authorized by any government agency for any specific system.

Architecture — The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time (IEEE STD 610.12). Three types of architectures are defined: operational, technical, and systems.

Architectural Oversight group (AOG) — The AOG is chaired by the DISA COE Chief Engineer and consists of a primary representative members from each Services/Agency using the COE, DISA COE management, and technical representatives for the above. This body has the responsibility for formulation of the top level architectural guidance for the COE and to ensure that the requirements of the Services/Agencies are addressed.

Client — A computer program, such as a mission application, that requires a service. Clients are consumers of data while servers are producers of data.

Client/Server — A particular kind of computing architectural model in which consumers (clients) and producers (servers) cooperate to create an application. Clients request services from servers, while servers may service one or more clients simultaneously. A typical example of a server is a database server. An example of a client is a software component that allows an operator to prepare a query, pass the query to the database, and then display the results to the operator.

Commercial Off-The-Shelf Software (COTS) — Software that is available commercially. Examples include versions of UNIX, X Windows, or Motif, as well as standard products such as Oracle and Sybase.

Common Operating Environment (COE) —The collection of standards, specifications, and guidelines, architecture definition, software infrastructure, reusable components, APIs, methodology, runtime environment definition, reference implementation, and methodology that establishes an environment on which a system can be built. The COE allows segments created by separate developers to function together as an integrated system. The COE is the vehicle that

assures interoperability through a reference implementation that provides identical implementation of common functions. It is important to realize that the COE is both a standard and an actual product (e.g., reference implementation) composed of reusable software components built according to a set of open standards and specifications.

COE-Component Segment — A segment that is contained within the COE. All software in COE-based systems is packaged as a segment, including those within the COE itself. Strictly speaking, "COE component" is a segment attribute rather than a separate segment type. Segments are specifically identified as COE components because specialized processing is performed on them during software installation, and they are handled more rigorously in the development cycle.

COE Developer — An agent tasked by the Government to develop COE function(s) for the purposes of integrating into the Defense Information Infrastructure Common Operating Environment

COE Kernel —That subset of the COE-component segments that is required on all platforms. As a minimum, this consists of the operating system, windowing software, security, segment installation software, and an Executive Manager. The COE is designed to minimize the size of the kernel so that minimal resources are required at each platform. Definition of the kernel is independent of whether the platform will be used as a database server, an applications server, or a client platform.

COE User — Any person or organization that physically loads and operates the COE capability to fulfill a mission requirement.

Component Segment — Those services (and standards) contained in the COE that perform the common functions necessary for any system. Examples include (but are not limited to): user interface services, security administration services, system administration services, data management services, track management services, and communications services.

Commercial-Off-The-Shelf (COTS) — Commercial software components employed within the COE product and requiring configuration management within the build. Examples include Motif, the X Window System, and SYBASE.

Compliance — An integer value, called the compliance level, which measures (a) the degree to which a segment or system achieves conformance with the rules, standards, and specifications described by the COE, (b) the degree to which the segment or system is suitable for integration with the COE reference implementation, and (c) the degree to which the segment or system makes use of COE services. Compliance is measured for segments and COE-based systems.

Compliance Category — One of the four areas (Runtime Environment, Style Guide, Architectural Compatibility, Software Quality) in which compliance is measured. These four categories form a spectrum for measuring compliance with regard to COE compatibility and degree of interoperability (Runtime Environment), user friendliness (Style Guide), product longevity (Architectural Compatibility), and program risk (Software Quality).

Compliance Level —The degree to which a segment is DII-compliant within a specific compliance category. Compliance levels are integer values only.

Composite Compliance — The compliance value assigned to a collection of segments. The purpose of a composite compliance value is to describe the degree of compliance a system achieves when it may contain COE-component segments that themselves are not Level 8 compliant. The composite compliance level for an arbitrary collection of segments is the compliance level of the least compliant segment.

Configuration Control Board (CCB) — The organization responsible for authorizing enhancements, corrections, and revisions to the COE, or to a COE based system. There is currently a Joint CCB to manage the COE and a Subscriber's CCB to manage the Maritime Common Systems Applications.

Core Component — A software capability which belongs in the core because it modifies, enhances, adds to, or replaces existing core services but has been temporarily packaged as a product which is custom installable into the COE outside the normal Segment installation process. Core components are developed because they provide core services that are undergoing evolutionary development making it prudent to limit distribution to a controlled set of target installations or because they add interfaces, data processing, and GUI capabilities in response to emergent requirements.

Core Software — A configuration of components of the COE to be used as a baseline for building a variant.

COE — That COE that is managed and maintained by the Defense Information Systems Agency (DISA) through the Joint CCB process and is utilized by all the Armed Services.

COE Component Segment — Those segments that are managed and maintained by DISA which are utilized by all the Armed Services.

Developer Fee — Annual fee payable to the CSDG by a program or organization that is sponsoring the development of segments to meet their specific mission requirements and using the COE and Common Systems Applications.

Engineering Change Proposal (ECP) — Engineering Change Proposals are submitted by subscribers to address engineering deficiencies in the system. ECP generated changes are reviewed by the Subscriber CCB prior to submission to DISA

Functional Description Document (FDD) — A Functional Description Document is prepared from a requirement submitted by the requesting activity and fully describes the requirement

Integration — The process of combining components, usually hardware and software, into a new, larger component to achieve some architectural requirement. Integration requires resolution of compatibility issues between components that are to be interconnected. Integration attempts to allow sharing of a common resource (such as data) without the need for intermediate translations from one format to another. Note that the COE is a technique for achieving integration that ensures interoperability.

Interoperability — 1. The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (DOD) 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JCS Pub 1-02)

Mission Application (or: Mission Segment) — Those services (and standards) NOT contained in the COE that perform mission specific functions as necessary for a particular user. Examples include (but are not limited to): Command and Control, Intelligence, Logistics, Transportation, Personnel, and Finance. A Mission Segment (not in the COE) should not be confused with a Component Segment (included in the COE). There will be both Joint Mission Segments (managed and maintained by DISA) and Maritime Mission Segments (managed and maintained by the individual Program Offices).

Near Real Time — Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JCS Pub 1-02)

Plug and Play — The ability for a COE-derived system to be scaled by the addition/removal of hardware or software components. To have the property of "plug and play," the system must be able to reconfigure itself automatically after component addition/removal with required human intervention limited to no more than a system power down or reboot.

Prototype Component Segment — A component segment candidate that is currently in development, but has not yet been accepted for inclusion in either the COE or as a maritime common systems application.

Real Time —Pertaining to the timeliness of data or information which has been delayed only by the time required for electronic communication. This implies that there are no noticeable delays. (JCS Pub 1-02)

Reusability — The ability of a software or hardware component, built to fulfill a requirement for a system built to achieve a particular mission, to be used to meet a similar requirement for another system that is being built to address a different mission need. Reusability allows system development and maintenance costs to be reduced because they can be shared across multiple programs. The COE contains a reuse strategy.

Segment — A collection of one or more software and/or data units most conveniently managed as a unit of functionality. Segments are defined from the perspective of an operator, not a developer, and are generally defined to keep related units together so that functionality may be easily included or excluded. They are usually defined as functional pieces (e.g., a word processor) that make sense from a system administrator perspective because segments are the lowest level components that can be installed on, or removed from, a platform.

Segment — A software application planned to operate as an addition to the COE and submitted in accordance with procedures specified by DISA. Segments must not duplicate, modify, enhance, or

extend areas preserved for core software functionality — mapping, data fusion, communications interfaces, peripheral control, printing, network alert management, and message composition and processing.

Segment Developer — an agent tasked by the Government to develop segments for the purposes of integrating into the COE.

Segmentation — The engineering process of decomposing system components into segments and creating the appropriate segment descriptor files. Proper segmentation is vital to a good system design and affects how well the component will operate in the resulting system.

Segment Compliance —The degree to which a segment, whether it is part of the COE or a mission application, is compliant. Compliance of individual segments is computed in order to calculate overall system compliance.

Server — A computer program that provides some service. Servers are producers of data while clients are consumers of data.

Shared Data Environment (SHADE) — The COE strategy and mechanisms for data sharing. SHADE includes the required data-access architectures, data sharing methodology, reusable software and data components, and guidelines, standards, and specifications for the development and migration of systems that meet the user's requirements for timely, accurate, and reliable data.

Software Change Proposal (SCP) — A SCP proposes a new functional requirement or operational capability.

Software Trouble Report (STR) — STRs address functional disparities between the specified operation of a system function or database and that exhibited by the system or product. STRs are generated by field operators, development activities, test and acceptance activities, the SSA, and developers. STRs may also address documentation and database discrepancies.

Subscriber — An activity that employs the baseline COE M as its system foundation and develops segments as applications.

System Compliance — The degree to which a COE-derived system in total meets COE standards, specifications, and rules. System compliance is a composite measure of all segments in the system whether they are part of the COE, or are application segments. The measure also includes provisions for components that are not COE-derived (e.g., mainframe components).

User Base Fee — Annual fee payable to the CSDG by a program or organization that is using the COE and Common Systems Applications. The User Base Fee is derived from the number of fielded sites; with a fielded site being defined as an operational installation.

Appendix O: Limited Release Agreement (LRA)

Per section 3B of this document, the following Limited Release Option required completion of a LRA:

- One-time Evaluator's Option
- Expanded Evaluator's Option
- IR&D Option

To utilize these options, one must meet the criteria for the selected option and agree to the restrictions/limitations on use of the COE development environment and document same by completing and signing the Limited Release Agreement provided on the following page.

Limited Release Agreement

Subject: Limited Release Agreement for the use of the COE

1. Purpose: This Limited Release Agreement (LRA) documents the terms under which the COE development environment has been provided and the limitations set forth concerning the use of said development environment.

2. Background: The COE concept contains the fundamental building blocks/architecture for DoD C2/C4I systems and defines an approach for building interoperable systems by specifying guidelines and standards by which the Services can reuse common existing software components and build new software in a seamless, automated fashion. PD-15E, the Navy Executive Agent for the COE, is responsible for managing and supporting the COE for the Maritime services and the supporting development community. In order to accomplish this tasking, a support infrastructure has been established along with the necessary cost sharing structure.

3. Agreements and Restrictions: The below specifies the recipient of the COE developmental software and the terms of the on which is agreement is based.

A. Company/Activity using COE Development Environment:

Name: _____
Address: _____
City/State/Zip: _____
POC Name: _____
POC Phone Number: _____
Program Supporting (if applicable): _____

B. Limited Release Option (select one):

____ One-time Evaluator's Option
____ Expanded Evaluator's Option
____ IR&D Option

C. Purpose for which the COE is being used (must meet the criteria of selected option above):

_____
_____
_____
_____

D. Software/Services to be provided for the option selected in paragraph 3B above are:

- One-time Evaluator's Option: This provides a one-time delivery of a requested development environment (software and available softcopy documentation) to the designated activity and 5-hours of telephone support during the first two weeks after

COE delivery to address installation issues and or basic development environment questions.

- Expanded Evaluator's Option: Expanded Evaluator's Option: This option provides requested development environment (software and available softcopy documentation), access to all updates for the remainder of the fiscal year (renewal required annually), up to 5-hours of telephone support to address installation issues and/or basic development environment questions.

- IR&D Option: This option provides requested development environment (software and available softcopy documentation), access to all updates for the remainder of the fiscal year (renewal required annually), up to 5-hours of telephone support to address installation issues and/or basic development environment questions.

E. Restrictions/Limitations on use of the COE provide under above options.
- The COE development environment/software is provide solely for the use of the activity/company specified in paragraph A and the purpose stated in paragraph C.
- Other than duplication of software to produce a "working copy", duplication of the provided COE software is prohibited.
- Distribution of the COE software to other parties, even within the same company/ activity, is prohibited.
- Any software developed under this Limited Release Agreement is not be used for operational purposes unless specifically authorized prototype evaluations.
- Any software developed under this Limited Release Agreement which is operationally fielded, other than above authorized prototypes, will require the developer or program to be considered a "standard COE subscriber". As such, it is subject to standard subscriber fee per paragraph 3A of the management plan and will be required to pay the remainder of the standard subscribers development fees for the fiscal years product was under development and the site fees for the year software was fielded.

4. Effective Dates: This services/software provided by the Navy COE EA in accordance with this LRA are effective for fiscal year ___, however, the restrictions and limitations stated in paragraph 3E will remain in effect indefinitely.

5. Approving Official: This document becomes official on the date signed:

_____
(signature/date)

_____
(title/position)

Appendix P: GCCS-M MOA Information

1. Points of Contact for GCCS-M Segments/MOA's are:

   - GCCS-M Segment Support for External Programs, Mr. Paul Nguyen, SSC SD 24222, (619) 553-4042, ptnguyen@spawar.navy.mil
   - GCCS-M External Interfaces, Mr. Douglas Anderson, PMW-157, (858) 537-0502, douglas.anderson@navy.mil
   - GCCS-M Chief Engineer, Mr. Chuck Schwartz, PMW-157, (858) 537-0601, charles.schwartz@navy.mil

2. Systems planning on integrating or interfacing with GCCS-M must obtain approval from PMW-157 and costs and responsibilities associated with this interface must be addressed in an MOA. Please contact the GCCS-M External Interfaces Manager (POC: Doug Anderson) to facilitate this process. An MOA will be required to delineate roles and responsibilities in regards to issues including software development, integration, testing, security, accreditation, etc.

The cost of obtaining GCCS-M software is $15K per fiscal year. This cost is not a license fee, it is a charge used to cover the costs associated with configuration management and software distribution. The $15K fee covers a copy of the requested GCCS-M software, an update copy of the software if released during applicable fiscal year, and a help desk support. Please note, an MOA is required before any software is released and is coordinated with the GCCS-M Software Support Activity (POC: Paul Nguyen). This MOA is valid for one fiscal year.