

**Concept of Operations
(CONOPS)
for the
Ordnance Information Systems
(OIS)**



OIS-CONOPS-1.0

Version 1.0

**Prepared by:
Naval Ammunition Logistics Center**

Table of Contents

Title	Page
RECORD OF REVISIONS AND/OR CHANGES	i
TABLE OF CONTENTS	iii
LIST OF FIGURES	vii
LIST OF APPENDICES	viii
LIST OF TABLES.....	ix
1. OVERVIEW.....	1
2. INTRODUCTION.	1
2.1 PURPOSE.....	1
2.2 SCOPE.....	1
2.3 OIS PROGRAM OBJECTIVES.....	1
2.4 OIS PROGRAM GOALS.....	2
2.5 BEST PRACTICES.	2
3. ORGANIZATIONAL RELATIONSHIPS.....	3
3.1 STRATEGIC STEERING BOARD (SSB).....	4
3.1.1 MEMBERSHIP, ROLES AND RESPONSIBILITIES.	4
3.2 ORDNANCE CIO.	5
3.2.1 ROLE.....	5
3.2.2 RESPONSIBILITIES.	5
3.3 PROJECT MANAGER.....	5
3.3.1 ROLES.....	6
3.3.2 RESPONSIBILITIES.	6
3.4 CONFIGURATION CONTROL BOARD (CCB).	7
3.4.1 MEMBERSHIP, ROLES, AND RESPONSIBILITIES.....	7
3.5 INTEGRATED PRODUCT TEAM(S).	7
3.5.1 MEMBERSHIP.	7
3.5.2 ROLES.....	7
3.5.3 RESPONSIBILITIES.	7

- 3.6 FUNCTIONAL USERS.8
 - 3.6.1 ROLES.8
 - 3.6.2 RESPONSIBILITIES.8
- 4. SYSTEMS MANAGEMENT APPROACH.8
 - 4.1 OIS PROGRAM LIFECYCLE.9
 - 4.1.1 REQUIREMENTS DEFINITION.9
 - 4.1.2 ANALYSIS.9
 - 4.1.3 DESIGN.9
 - 4.1.4 IMPLEMENTATION.9
 - 4.1.5 TESTING.10
 - 4.1.6 DEPLOYMENT.10
 - 4.1.7 MAINTENANCE.10
 - 4.2 OIS SYSTEMS MANAGEMENT.10
 - 4.2.1 REQUIREMENTS MANAGEMENT.10
 - 4.2.1.1 POLICY.11
 - 4.2.1.2 IMPLEMENTATION GUIDELINES.11
 - 4.2.1.3 REQUIREMENTS SPECIFICATIONS.11
 - 4.2.1.4 REQUIREMENTS MANAGEMENT OBJECTIVES.11
 - 4.2.2 PROJECT PLANNING.12
 - 4.2.2.1 POLICY.12
 - 4.2.2.2 IMPLEMENTATION GUIDELINES.12
 - 4.2.2.3 PLANNING REQUIREMENTS.13
 - 4.2.2.4 PROJECT PLANNING OBJECTIVES.13
 - 4.2.3 PROJECT TRACKING.14
 - 4.2.3.1 POLICY.14
 - 4.2.3.2 IMPLEMENTATION GUIDELINES.14
 - 4.2.3.3 PROJECT TRACKING REQUIREMENTS.14
 - 4.2.3.4 PROJECT TRACKING OBJECTIVES.15
- 5. CONFIGURATION MANAGEMENT.15
 - 5.1 CONFIGURATION IDENTIFICATION.15
 - 5.2 CHANGE CONTROL.16

5.3	CONFIGURATION STATUS ACCOUNTING.....	16
5.4	CONFIGURATION AUDITS.....	16
5.5	CONFIGURATION MANAGEMENT APPROACH.....	16
5.5.1	POLICY.....	16
5.5.2	IMPLEMENTATION GUIDELINES.....	16
5.5.3	CONFIGURATION MANAGEMENT REQUIREMENTS.....	17
5.5.4	CONFIGURATION MANAGEMENT OBJECTIVES.	17
6.	QUALITY ASSURANCE.....	18
6.1	QA ACTIVITIES.	18
6.1.1	PLAN DEVELOPMENT.....	18
6.1.2	STANDARDS AND PROCEDURES DEVELOPMENT.....	18
6.1.3	PROJECT AUDITING.....	18
6.1.4	REVIEW NOTIFICATION.....	18
6.1.5	SOURCE CODE MAINTENANCE.....	18
6.1.6	CHANGE DOCUMENTATION.....	18
6.1.7	RESOLUTION REPORTING.....	19
6.1.8	ANALYSIS AND DESIGN REVIEWING.	19
6.1.9	TEST PLAN REVIEWING.....	19
6.1.10	TEST EXECUTION VERIFICATION.	19
6.2	QUALITY ASSURANCE APPROACH.....	19
6.2.1	POLICY.....	19
6.2.2	IMPLEMENTATION GUIDELINES.....	19
6.2.3	QUALITY ASSURANCE REQUIREMENTS.....	20
6.2.4	QUALITY ASSURANCE OBJECTIVES.....	20
7.	DOCUMENTATION REQUIREMENTS.	20
7.1	PURPOSE OF SOFTWARE LIFE CYCLE DATA.....	20
7.2	OPERATIONS OF SOFTWARE LIFE CYCLE DATA.....	21
7.3	CHARACTERISTICS OF SOFTWARE LIFE CYCLE DATA.....	21
7.4	BASIC TYPES OF SOFTWARE LIFE CYCLE DATA.	22
7.5	PRESENTATION FORM OF SOFTWARE LIFE CYCLE DATA.....	22
7.6	DoD INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP).....	23

8. REFERENCES/ACRONYMS/DEFINITIONS.....23

8.1 REFERENCES.....23

8.2 ACRONYMS.....24

8.3 DEFINITIONS.....24

DOCUMENT IMPROVEMENT PROPOSAL

List of Figures

Title	Page
FIGURE 1, OIS ORGANIZATIONAL RELATIONSHIPS.....	4

List of Appendices

Title	Page
COMMENT SUMMARY	A-1
OIS SSB CHARTER.....	B-1
OIS CCB CHARTER.....	C-1

List of Tables

Title	Page
TABLE 1, CUSTOMER COMMENT SUMMARY	A-1
TABLE 2, OIS PROJECT RESPONSE COMMENT SUMMARY	A-2

1. Overview.

This Concept of Operations (CONOPS) sets forth the framework for managing the Ordnance Information Systems (OIS) Program and provides guidance on the roles and responsibilities of the various participants. The systems management approach is presented and key components discussed.

2. Introduction.

The OIS Program encompasses the management of NAVAMMOLOGCEN-sponsored automated information systems used throughout the Navy and Marine Corps for ordnance asset management and accountability.

2.1 Purpose.

The purpose of this CONOPS is to:

- a. Specify how the Ordnance Chief Information Officer (CIO) will ensure the various systems are effectively managed and supported.
- b. Define the roles and responsibilities.
- c. Define the OIS Program organization and management approach.

2.2 Scope.

The scope of the CONOPS applies to all ordnance management-related software development projects under the cognizance of the NAVAMMOLOGCEN OIS Program. These projects include centrally managed application software, development tools databases, and training. It does not include DoD managed communication networks, Navy Wide Area Networks (WANs) and Local Area Networks (LANs).

2.3 OIS Program Objectives.

The objectives of the OIS Program are to:

- a. Effectively integrate the NAVAMMOLOGCEN-sponsored ordnance information system projects.
- b. Promote efficient OIS management and data integrity, interoperability, portability, and scalability.
- c. Re-engineer processes to effect maximum use of system to reduce manual intervention.
- d. Migrate and optimize Navy ordnance legacy systems and promote a seamless interface between Navy and DOD systems.

- e. Migrate the OIS from vendor-dependent and sole-source environments to the DOD-mandated Open Systems Environment (OSE).
- f. Become Defense Information Infrastructure (DII) and Common Operating Environment (COE) compliant.

2.4 OIS Program Goals.

The OIS Program goals are to:

- a. Gain customer involvement and support in defining requirements.
- b. Provide users with reliable and accessible data.
- c. Ensure the program fully supports user requirements.
- d. Promote high functionality and system performance.
- e. Provide effective program management.
- f. Provide process for program review and improvement.
- g. Effectively integrate the man-machine interface.
- h. Reduce data transmission of database changes to absolute minimum.
- i. Reduce to the absolute minimum the number of individuals that need to write to the database.
- j. Reduce cycle time of program development and upgrades.

2.5 Best Practices.

The OIS Program will avoid imposing government-unique requirements that significantly increase industry compliance costs for systems development. Practices designed to make the process easier include: Integrated Product and Process Development (IPPD) performance-based specifications, management goals, reporting and incentives; open systems approach (that emphasizes commercially supported practices, products, specifications, and standards); realistic cost estimates and cost objectives; best value evaluation and award criteria; use of past performance in source selection; results of software capability evaluations; government-industry partnerships; and the use of pilot programs to explore innovative practices.

3. Organizational Relationships.

Figure 1 identifies the organizational relationships associated with the OIS Program. The activities represented include program guidance, program direction and oversight, management, requirement change approval and execution.

The Ordnance CIO receives strategic guidance from the Strategic Steering Board (SSB). The SSB approves the OIS strategic plan and ensures that the ordnance community functional requirements are satisfied by the OIS Program. The SSB is chaired by NAVSUP (NAVAMMOLOGCEN) and has members from the OPNAV staff, Fleet CINCs, Marine Corps, NAVSEA, Coast Guard, NAVSPECWARCOM and invited participation from Department of the Navy (DON) ordnance program offices and the OIS Project Managers.

The Ordnance CIO is responsible for overall program planning and gives OIS project direction and oversight to OIS Project Managers who manage and execute their projects.

The Ordnance CIO is supported by the OIS Configuration Control Board (CCB) and Integrated Product Teams (IPTs). The CCB reviews and approves/disapproves proposed changes or modification to existing products or processes submitted from the user community. An IPT is established at the Ordnance CIO's discretion when a task requires a specialized group to address a requirement or element of the OIS Program.

The SSB, Ordnance CIO, Project Managers, CCB and IPT(s) receive input and feedback at various levels from the ordnance functional user community.

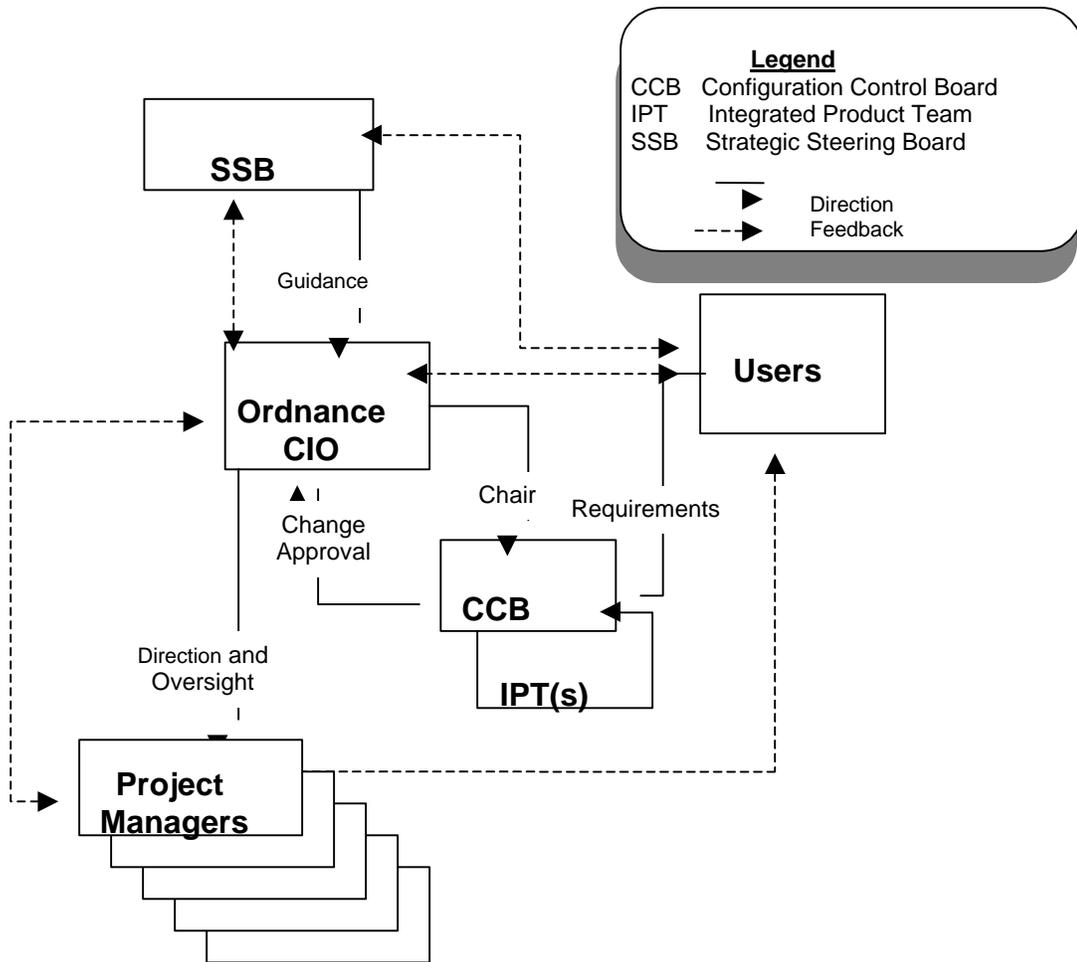


Figure 1, OIS Organizational Relationships

3.1 Strategic Steering Board (SSB).

The SSB is the senior management group that approves the OIS Program Strategic Plan and provides guidance to OIS project change control.

3.1.1 Membership, roles and responsibilities.

Membership, roles, and responsibilities are defined in the OIS SSB Charter. The draft charter is included in Appendix B -- OIS SSB Charter.

3.2 Ordnance CIO.

The Ordnance CIO has oversight and overall responsibility for the program management of the OIS Program. The Ordnance CIO sets policy and direction for the development and maintenance of the projects.

3.2.1 Role.

The Ordnance CIO provides OIS program management.

3.2.2 Responsibilities.

The Ordnance CIO is responsible for:

- a. Program Planning – Preparing the overall program plan and coordinating the OIS Program Strategy with the SSB.
- b. Joint Service Coordination - Participating as the Navy's principal agent on all Joint Service ordnance information systems and requirements.
- c. System Management – Overseeing the OIS management, including the system life cycle phases: requirements definition, analysis, design, development, testing, deployment, and maintenance.
- d. Systems Maintenance – Preparing annual reports to the SSB on program performance and providing briefings and/or reports, as required.
- e. CCB and IPT Direction – Providing CCB and IPT direction.
- f. Program Budgeting – Managing the budget for the OIS Program.
- g. Testing – Ensuring test plans are properly developed and executed.
- h. Configuration Control – Ensuring that system configuration control is properly executed.
- i. Quality Assurance (QA) - Ensuring quality control is executed at every level of systems management.
- j. Contingency Planning – Ensuring contingency planning needs are met.
- k. Documentation – Ensuring system documentation is properly maintained.

3.3 Project Manager.

Project Managers should efficiently and effectively manage the life cycle development of assigned projects.

3.3.1 Roles.

Project Managers serve as:

- a. Project Planner.
- b. Funds Manager.
- c. CCB Member (non-voting).

3.3.2 Responsibilities.

Project Manager(s) are responsible for:

- a. Project Planning – Providing project plan to the Ordnance CIO for approval.
- b. Funds Execution – Ensuring funds are executed in accordance with approved plan.
- c. Project Management – Providing project analysis and control using program metrics in support of the assigned project to evaluate and select alternatives, measuring progress, and documenting design decisions to include:
 - (1) Conducting trade-off studies among requirements (operational, functional, and performance);
 - (2) Establishment of risk management;
 - (3) Configuration management process to control project products, processes, and related documentation in accordance with the approved Configuration Management Plan; and
 - (4) An approved integrated data management system to capture and control the technical baseline (configuration documentation, technical data, and technical manuals), provide data correlation and traceability among requirements, designs, decisions, and rationale to serve as a ready reference.
- d. Testing - Ensuring project test plans are properly developed and executed according to the approved test procedures.
- e. QA - Ensuring quality control is executed at every level of project management.

3.4 Configuration Control Board (CCB).

The CCB is the group that reviews proposed system changes from the user community, evaluates internal and external system(s) impacts, evaluates change resource requirements, and approves requested changes as requirements.

3.4.1 Membership, roles, and responsibilities.

Membership, roles, and responsibilities are defined in the OIS CCB Charter. The draft charter is included in Appendix C -- OIS CCB Charter.

3.5 Integrated Product Team(s).

An IPT is established at the Ordnance CIO's discretion when a task requires a specialized group to address a requirement or element of the OIS Program. The IPT(s) will function in a spirit of teamwork with participants empowered and authorized, to the maximum extent possible, to make commitments for the organization or the functional area they represent. The objective of the IPT is to efficiently and effectively manage and complete tasks assigned by the Ordnance CIO.

3.5.1 Membership.

CCB members and participants may serve as members on IPT(s).

3.5.2 Roles.

The IPT provides:

- a. Project functional evaluation.
- b. Support for development, test and maintenance.
- c. Documentation and training review.

3.5.3 Responsibilities.

The IPT is responsible for providing:

- a. Assistance in strategy development and program planning.
- b. An IPT plan of action and milestones.
- c. Activity coordination.
- d. Issue resolution and recommendation.
- e. SCRs for potential improvements that address identified deficiencies.

3.6 **Functional Users.**

Functional users provide the primary input to help determine required system functionality. This is accomplished by the user's continuous responsive feedback to the technical community through the CCB.

3.6.1 **Roles.**

The functional users provide:

- a. Functional evaluation.
- b. Requirements origination.
- c. User interaction and feedback.

3.6.2 **Responsibilities.**

Functional users are responsible for:

- a. Submitting System Change Requests (SCRs) to the CCB for review and approval/disapproval. SCRs are used to identify system operational and functional improvements.
- b. Providing system evaluation and feedback to the CCB. User feedback provides first-hand system performance information that is essential to effective system maintenance.

4. **Systems Management Approach.**

The objectives of the OIS systems management approach and methodologies are outlined to support management policies for the following areas:

- Requirements Management
- Planning
- Tracking
- Configuration Management
- Quality Assurance

These management areas form the core of the methodology for OIS Program Management of the OIS Program lifecycle. Paragraphs 4.2, 5.0 and 6.0 provide the OIS approach and policy for each of these areas.

4.1 OIS Program Lifecycle.

The OIS Program encompasses the following lifecycle phases: Requirements Definition, Analysis, Design, Implementation, Testing, Deployment, and Maintenance. The following paragraphs summarize each of the OIS Program Lifecycle phases. The specific requirements and tasks for each lifecycle phase are detailed in the OIS Program Software Engineering Process (SEP) Standard.

4.1.1 Requirements Definition.

During requirements definition, the user will identify and communicate the functional requirements of the system. System changes will be in accordance with the OIS Configuration Management Policies and Procedures and the OIS Program Standard Operating Procedures document. Requirements determination and requirements specification development will be in accordance with the OIS SEP Standard which details the procedures to be followed for determining and managing requirements.

4.1.2 Analysis.

During analysis, each approved system change or enhancement in response to system requirements will be analyzed to the lowest detail, and will include the following:

- classification of the requirement or requested change
- assessment of the requirement/change objectives, constraints, scope, and specification
- impact (and estimates) on the program schedule, budget, and resources

4.1.3 Design.

The OIS Program Design Team will develop system designs within the guidance provided by the SSB, by direction of the OIS CIO, and by approved changes. The design changes may affect any aspect of the system including processing logic, database design, and screen interface.

4.1.4 Implementation.

The OIS CIO and Project Managers will ensure implementation of the approved changes. Configuration control is a crucial element of the implementation phase. Reference paragraph 5.0, Configuration Management, and paragraph 6.0 Quality Assurance, for appropriate controls to include restricted access to source code, modification verification, and change documentation.

4.1.5 Testing.

Each system element will be thoroughly tested. Test levels are identified as follows, the most extensive testing will focus on the application software of each system:

- Unit testing
- Module testing (Unit integration)
- Application testing
- System testing
- Acceptance testing

Extensive application testing will ensure that the system and system changes have been effectively and efficiently implemented. Test Plans, Test Descriptions and Test Results will be used to document test scenarios and to verify that the system satisfies the specified functional and technical performance criteria. The development and test phases are complete when the systems have successfully executed the Test Plan. Check-off lists will be used to verify that tests are successfully completed.

4.1.6 Deployment.

After successful testing, deployment is executed by the Project Managers in accordance with the documented deployment plans. The deployment process includes pre-deployment preparation, distribution, equipment baseline configuration identification, and application installation, database load, acceptance testing, acceptance, training, and post-implementation support. Each of these activities is tailored in accordance with the scope, complexity, and strategy of succeeding version releases.

4.1.7 Maintenance.

Maintenance of the system is executed by the Project Managers in accordance with OIS CIO direction and shall be in keeping with the OIS Program Strategic Plan. Maintenance includes application software fixes and improvements, hardware and operating software architecture upgrades, and all related documentation.

4.2 OIS Systems Management.

The following paragraphs provide the OIS management policies for OIS Program Management areas.

4.2.1 Requirements Management.

Requirements establish and provide a common means for maintaining an understanding and agreement of the system capabilities. Requirement statements form the basis for estimating, planning, performing, and tracking activities and are critical to obtaining system acceptance.

The purpose of requirements management is to ensure that the system requirements form the basis for all planning and development efforts and that requirements and changes to requirements are managed throughout the system lifecycle.

The following paragraphs provide the OIS approach for requirements management.

4.2.1.1 Policy.

The requirements management policy requires that all OIS projects and changes include a clearly defined problem statement with defined technical and non-technical requirements that provide the solution to satisfying a documented need. Requirements must be thoroughly documented and understood by the CCB and development team. Changes to requirements must be managed throughout the system lifecycle.

4.2.1.2 Implementation Guidelines.

Requirements definition is one of the most critical steps in the process of developing a system and/or implementing a system change. Without well-defined requirements, project managers cannot plan, developers will not understand what to build, customers will not know what to expect, and it will be difficult to validate (i.e., test) whether the original need has been satisfied.

The Project Manager is responsible for ensuring that technical requirements are defined in accordance with the requirements evaluation factors detailed in the OIS SEP Standard and that functional requirements are met.

4.2.1.3 Requirements Specifications.

Requirements specifications will be developed to document all requirements of the system or system change. Any additional information with regard to requirements derived during lifecycle stages will be documented. Requirements specifications will vary from system to system based on size, complexity, etc. and the degree of specification and the formality of the specification will also vary.

At a minimum, each project will have an approved need statement and a means of requirements traceability. Full requirements specifications will be developed in accordance with the OIS SEP Standard.

4.2.1.4 Requirements Management Objectives.

The OIS objectives for requirements management are as follows. The project manager must ensure compliance to the overall requirements management policy.

- a. Ensure that system requirements provide a clearly stated, verifiable, and testable foundation for development and management of the project, based on technical and non-technical requirements.

- b. Ensure that the scope of an effort is defined by the system requirements and that these requirements form the basis for all plans, products, and activities.
- c. Ensure that team members thoroughly understand requirements prior to any development efforts.
- d. Record initial requirements and review/assess the impact of all changes to the initial requirements throughout the system lifecycle.
- e. Track and document all changes to requirements and update all necessary system documentation affected by the change.
- f. Define, collect, and store metrics (measurements) associated with the requirements phase.

Compliance to the requirements management policy is demonstrated by the following system artifacts being made available on demand:

- Requirements statement and objective
- System Requirements Document
- Requirements traceability

4.2.2 Project Planning.

Project planning includes developing estimates for the work to be performed, establishing the necessary commitments, and defining the plan to perform the work. The project plans will address the commitments in terms of resources, constraints, and capabilities of the project and provides the basis for guiding the management and the performance of the project and evaluating progress. The purpose of project planning is to ensure proper planning is performed for successful project completion.

The following paragraphs provide the OIS approach for project planning.

4.2.2.1 Policy.

The project planning policy requires that a documented plan be maintained and followed for each system. The project planning document defines project goals, processes, and provides resource estimates (in terms of schedule, cost and development). The project plan will be updated throughout the system lifecycle to accurately reflect the current plan.

4.2.2.2 Implementation Guidelines.

Project planning defines the work to be performed and describes how the tasks will be executed. Planning begins with a definition of the specific work to be performed (based on the documented requirements) and other constraints and goals that define and bind the project. The project plans will include estimates for size, technical scope of effort, and

resources required to complete the project. Results from effective planning will be a project schedule, identification and assessment of risks, and negotiation of commitments.

The Project Manager is responsible for developing, implementing, and maintaining the project plan. Detailed steps and tools are outlined in the OIS SEP Standard.

4.2.2.3 **Planning Requirements.**

The project plan forms the basis for management efforts associated with the project. Project planning requirements will vary between systems and are typically determined by the size, cost, and complexity. Project managers are encouraged to add to and tailor the planning methodology to include additional elements as the size, cost, and complexity increases. At a minimum, each system will have a project plan that addresses:

- a. Project deliverables.
- b. Sequence of tasks to be performed.
- c. Schedule of all tasks to be performed.
- d. Dependency relationships between tasks.
- e. Resources required to complete the project.
- f. Project estimate and budget.
- g. Development organization.
- h. Project risk assessment.
- i. Process for ensuring quality.
- j. Process for configuration management.

4.2.2.4 **Project Planning Objectives.**

The OIS objectives for project planning are as follows. The project manager must ensure compliance to the overall project planning policy.

- a. Develop a plan for each system that appropriately and realistically covers the activities and commitments (based on documented requirements). The plan should break down the development effort into manageable components.
- b. Ensure that all affected groups and individuals (e.g., developers, users, etc.) understand the planning estimates and assignments and commit to support them.
- c. Document all approved estimates and plans for tracking activities and commitments. Define project estimates throughout project lifecycle phases.

Compliance to the project planning policy is demonstrated by the following system artifacts being made available on demand:

- Project schedule with milestones
- Project estimates
- List of deliverables
- Work Breakdown Structure

4.2.3 **Project Tracking.**

Project tracking involves monitoring and reviewing the project accomplishments and results against documented estimates contained in the project plan, and adjusting these estimates based on the actual accomplishments and results. The project planning document for the effort is used as the basis for tracking activities, communicating status and revising plans. Regular technical and management reviews will be conducted to ensure that the management and development personnel are aware of the project status and plans, and that issues and action items receive appropriate attention.

The following paragraphs provide the OIS approach for project tracking.

4.2.3.1 **Policy.**

Project tracking requires that project managers continuously track and monitor progress against the project plan. The project manager is responsible for implementing the project tracking policy.

4.2.3.2 **Implementation Guidelines.**

The project plan serves as the basis for the project's monitoring, controlling, and reporting activities. By following the plan and gathering relevant data for status meetings and reports, information will be available to accurately identify issues and problems early, minimize project risks, and monitor, control, and report progress.

4.2.3.3 **Project Tracking Requirements.**

Projects often fail due to inattention to basic control principles. Many times a project team is too busy completing the project and not enough time is spent tracking status and anticipating potential problems.

Project tracking requirements will vary by system based on the size, cost, and complexity. The formality of project tracking may change based on the system requirements. Project managers may tailor the project tracking methodology as appropriate to that of the development environment.

At a minimum, each system will follow a project tracking methodology that addresses the following:

- a. Track and monitor project activities to measure actual performance against planned performance.
- b. Review and communicate status and future actions on both formal and informal basis.
- c. Monitor and mitigate potential problems to reduce the likelihood of occurrence.
- d. Establish a tracking process that includes a central repository for project issues and action items that are addressed in a timely manner.

- e. Establish a corrective action process to document and track plans to correct an issue or action item that impacts the documented plan and to establish a baseline for re-planning.

4.2.3.4 **Project Tracking Objectives.**

The OIS objectives for project tracking are as follows. The project manager must ensure compliance to the overall project tracking policy.

- a. Ensure that actual results and performance of the project are regularly tracked against documented and approved plans.
- b. Ensure that risk assessment is performed during key points in the project.
- c. Ensure that corrective action is taken when the actual results and performance of the project deviate from the plans.
- d. Ensure that changes to commitments are understood and agreed to by all affected groups and individuals.

Compliance to the project tracking policy is demonstrated by the following system artifacts being made available on demand:

- Reports on actual vs. estimated cost.
- Reports on actual vs. planned schedule.
- Risk analysis.
- Status reports
- Corrective action plans (as required)

5. **Configuration Management.**

The purpose of Configuration Management (CM) is to establish and maintain the integrity of the systems throughout their life cycles. The process involves the identification of configuration baselines and the establishment of procedures to systematically control changes, thereby maintaining the traceability of the configuration throughout the hardware/software life cycles. OIS CM will follow the procedures specified in the approved OIS CM Plan. Key configuration management areas are detailed below.

5.1 **Configuration Identification.**

Configuration identification is the process of determining and defining the system configuration. The configuration is defined in terms of individual Configuration Items (CIs). CIs initially consist of documentation and, as implementation occurs, actual system components such as hardware, software and data communication equipment. In this process, CIs are identified by the Project Manager and, if approved by the Ordnance CIO, released as baseline CIs.

5.2 Change Control.

The Ordnance CIO oversees the review and approval process for functional changes. All proposed changes are documented. Once a change is approved, the implementation of the modification is governed by the OIS CM Plan change control process.

5.3 Configuration Status Accounting.

A configuration status accounting system is an essential component of configuration management. This system provides traceability and status information within the CM process. A configuration status accounting system is used to document CIs progression throughout the life cycle, provide communication and feedback, and provide up-to-date information on SSB guidance and Ordnance CIO directives.

Configuration status accounting assures that the approved configuration (i.e., the baseline) and the status of any pending changes to the baseline is documented.

5.4 Configuration Audits.

The purpose of configuration audits is to determine whether the evolving system complies with specified standards and original project objectives through examination of the products and technical documentation. Auditing procedures can include both formal and informal verifications.

5.5 Configuration Management Approach.

CM involves identifying project baseline items, controlling these items and changes to them, and recording and reporting status and change activity for these items. Changes to the baseline items are controlled systematically using the OIS defined change control process. The configuration of a system or any of the controlled products can be distinctly identified at any point in time.

5.5.1 Policy.

The CM policy requires that CM be performed in accordance with OIS established CM procedures to ensure that controlled and stable baselines are established for planning, managing, and developing systems. As part of this process, the integrity of the system configuration is controlled over time, and the status and content of the baselines are known.

5.5.2 Implementation Guidelines.

CM is a formal discipline that provides developers and users with the methods and tools to identify the system developed, establish baselines, control changes to baselines, record and track status, and audit the system. During the planning process, the procedures and required resources for CM will be defined and the CIs that require tracking will be identified. CM planning is performed to:

- a. Assign authority and responsibility for CM for the project.

- b. Ensure that CM is implemented throughout the system life cycle by setting standards, procedures, and guidelines that are produced and distributed to the development team.
- c. Ensure the establishment of a repository for storing CIs and associated CM records.
- d. Ensure that reviews of baselines and CM activities occur on a regular basis.
- e. Ensure that changes are controlled and that the impact of change to CIs is understood prior to approving a change.

5.5.3 Configuration Management Requirements.

A CM plan will either be included as part of the project plan, be maintained as a separate document, or maintained as sections within an overall quality plan. The degree of specification of the CM plan is dependent on the system size, cost, and complexity. Project Managers are encouraged to tailor the methodology to develop CM processes that are appropriate to the system.

5.5.4 Configuration Management Objectives.

The OIS objectives for CM are as follows. The project manager must ensure compliance to the overall CM policy.

- a. Explicitly assign responsibility for CM for each project.
- b. Ensure that each system has a CM plan.
- c. Ensure CM work is performed according to the project plan.
- d. Ensure that CM is implemented on products throughout the system life cycle.
- e. Ensure that all systems have a repository for storing CIs and associated CM records.
- f. Ensure that quality assurance audits of the baselines and CM activities are performed on a regular basis.

Compliance to the CM policy is demonstrated by the following system artifact being made available on demand:

- A CM plan (system-specific or for overall development organization).

6. Quality Assurance.

Quality Assurance (QA) is the process of evaluating, reviewing, and auditing the quality and effectiveness of an information system. The purpose of QA is to provide appropriate visibility into the process being used by the development team and of the products being built. A QA Plan is begun in the early stages of a system's development where quality requirements set forth by management, system developers, and the user community are documented. The QA Plan is further refined throughout the deployment phase of the completed information system. OIS projects will conform to the approved OIS QA Plan.

6.1 QA Activities.

The following paragraphs describe the minimum QA activities performed on OIS projects.

6.1.1 Plan Development.

The QA Plan determines the activities to be included in the QA process. The agent responsible for the group being evaluated manages and ensures the execution of the QA plan (e.g., the Project Manager is responsible for the QA activities of his system).

6.1.2 Standards and Procedures Development.

Standard QA procedures will be used as the guideline for the QA reviews and audits. These standards and procedures verify that the project adheres to the OIS Program requirements.

6.1.3 Project Auditing.

Project activities will be reviewed and system performance audits will be conducted throughout the system's life cycle. Results of these reviews and audits provide feedback to management.

6.1.4 Review Notification.

Affected groups or individuals will be notified of planned QA activities and the results of such activities. The groups or individuals will be familiar with QA goals and values.

6.1.5 Source Code Maintenance.

Source code will be developed and maintained in accordance with OIS CM and QA policies and procedures.

6.1.6 Change Documentation.

All change requests will be documented and tracked in accordance with OIS CM and QA policies to closure to ensure that all changes and requests for changes have been addressed.

6.1.7 Resolution Reporting.

All non-compliant issues will be reported to project or program management for resolution.

6.1.8 Analysis and Design Reviewing.

Systems analyses and design methodologies and approaches will have full concurrence by the Ordnance CIO. Requirements specifications and system design documents will be prepared and submitted to the Ordnance CIO/Project Manager for concurrence.

6.1.9 Test Plan Reviewing.

Test plans will be developed and submitted to the OIS CIO/Project Manager for concurrence.

6.1.10 Test Execution Verification.

A checklist will be used to verify that all required levels of testing (unit, module, application, system and acceptance testing) are completed to ensure that multiple systems work together.

6.2 Quality Assurance Approach.

QA involves reviewing and auditing the products and activities to verify that they comply with the applicable OIS procedures and standards. Project Managers are responsible for the implementation of the QA policy in their respective systems.

6.2.1 Policy.

The QA policy requires that QA be performed in accordance with OIS established QA procedures to ensure product quality.

6.2.2 Implementation Guidelines.

During the planning process, the procedures and required resources for QA will be defined in the OIS or system QA Plan. QA planning is performed to:

- a. Assign authority and responsibility for coordinating and implementing QA for the project.
- b. Ensure QA plan is developed in accordance with OIS QA policies and procedures.
- c. Ensure QA activities are performed in accordance with the QA plan.
- d. Ensure that affected groups and individuals are informed on QA activities and results.
- e. Verify QA compliance of development activities.
- f. Review and audit products with the QA group to verify compliance.

6.2.3 Quality Assurance Requirements.

A QA plan will either be included as part of the project plan, be maintained as a separate document, or maintained as sections within an overall quality plan.

6.2.4 Quality Assurance Objectives.

The OIS objectives for QA are as follows. The project manager must ensure compliance to the overall QA policy.

- a. Ensure that all QA activities are planned and approved.
- b. Ensure that all development activities and products adhere to QA plans, standards, procedures and requirements.
- c. Ensure that all affected groups and individuals are informed of QA activities and results.
- d. Ensure that noncompliance issues that cannot be resolved within the project are presented to senior management for resolution.

7. Documentation Requirements.

Documentation is considered essential to effectively develop, deploy, and maintain the OIS Program projects. The documentation serves as a program and project management tool, which must be generated and maintained throughout each project life cycle. Documentation shall be developed using IEEE/EIA 12207, Information Technology – Software Life Cycle Processes.

There are basic principles to be considered in preparing data during the execution of the software life cycle processes of IEEE/EIA 12207.

7.1 Purpose of Software Life Cycle Data.

The life cycle data should support the following actions:

- a. Describe and record information about a software product during its life cycle;
- b. Assist usability and maintainability of a software product;
- c. Define and control life cycle processes;
- d. Communicate information about the system, software product or service, and project to those who need it;
- e. Provide a history of what happened during development and maintenance to support management and process improvement;

- f. Provide evidence that the processes were followed;
- g. Assist the software logistics planning (i.e., replication, distribution, installation, training) for a software product;
- h. Provide data change history.

7.2 Operations of Software Life Cycle Data.

The life cycle data should be supported by the following operations:

- a. Create
- b. Read
- c. Update
- d. Delete
- e. Archive
- f. Distribute
- g. Transition (transfer of data and ownership/usage rights).

7.3 Characteristics of Software Life Cycle Data.

The life cycle data should adhere to the following characteristics:

- a. Unambiguous: Information is unambiguous if it is described in terms that only allow a single interpretation, aided, if necessary, by a definition. It implies having the characteristic of being understandable by intended users.
- b. Complete: Information is complete if it includes necessary, relevant requirements and/or descriptive material, responses are defined for the range of valid input data, and terms and units of measure are defined.
- c. Verifiable: Information is verifiable if it can be checked for correctness by a person or tool.
- d. Consistent: Information is consistent if there are no conflicts within it. It also should include consistency between related data and conformity of data.
- e. Modifiable: Information is modifiable if it is structured and has style such that changes can be made completely, consistently, and correctly while retaining the structure.
- f. Traceable: Information is traceable if the origin of its components can be determined.
- g. Presentable: Information is presentable if it can be retrieved and viewed. It implies having the characteristic of being understandable by intended users.
- h. Secure and private: Information is secure and private if there is controlled access to the information.

- i. Protected: Information is protected if there is persistence in data backup and protection from loss or damage.
- j. Accurate: Information is accurate if it is correct and adequate.

7.4 Basic Types of Software Life Cycle Data.

The life cycle data should contain content in the following areas:

- a. Requirements data: Expected functionality, operational context, performance constraints and expectations, basis for qualification testing, and key decision rationale.
- b. Design data: Architecture, algorithms, design constraints, mapping to requirements, and key decision rationale.
- c. Test data: Test strategy and criteria, cases (what to test), procedures (how to carry out tests), test results, and key decision rationale. Test data should include a mapping to requirements.
- d. Configuration data: Configuration description, build instructions, reference to source code, reference to object code, data integrity approach, description of development environment, and key decision rationale.
- e. User data: Software overview, system access information, commands and responses, error messages, operational environment, and key decision rationale. User data should include help systems, training material, and operational logs.
- f. Management data: Management plans, status reports, management indicators, criteria and key decision rationale, and contract and other procurement information. Management data should include management and technical risks.
- g. Quality data: Quality plans and procedures, corrective action status, root cause analysis, product quality characteristics and process measurement data, and criteria and key decision rationale.

7.5 Presentation Form of Software Life Cycle Data.

The presentation form of life cycle data should:

- a. Be appropriate to support the purpose of the life cycle data;
- b. Support the retrieval and review of data of a software item during its life cycle;
- c. Support the basic operations on data of a software item during its life cycle; and
- d. Be selected subject to concurrence of the users of the data.

Note: In preparing the final contract, the acquirer should specify the requirements for data delivery, taking into account the maintenance strategy. Some of the choices are:

- a. Raw data – Repositories of the development tools such as Computer Aided Software Engineering (CASE) tools, databases, file systems, and other tool repositories.
- b. On-line publishing systems – Data assembled and formatted for presentation by systems such as: word processors, World Wide Web publishing and display systems, Second Generation Markup Language (SGML) viewers.
- c. Hard copy print – traditional paper document form.

7.6 DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

The objective of DITSCAP is to establish a DoD standard infrastructure-centric approach that protects and secures the entities comprising the Defense Information Infrastructure (DII). The activities presented in the DITSCAP standardize the Certification and Accreditation (C&A) process for a single information technology (IT) entity that leads to more secure system operations and a more secure DII. This process supports the infrastructure orientation for entity systems, with a focus on the mission, environment, and architecture for those systems. For a system in development, the intent is to identify appropriate security requirements, design to meet those requirements, test the design against those same requirements, and then monitor the accredited system for changes or re-accreditation as necessary.

DITSCAP applies to Information Technology Security (ITSEC) certification and accreditation professionals, users, acquisition and maintenance organizations, developers, system integrators, and procurement officials. Each of these communities has a specific role in developing, procuring, employing, and operating an information system with an acceptable level of residual risk.

8. References/Acronyms/Definitions.

8.1 References.

- a. DoD Directive 5000.1, "Defense Acquisition," 1996
- b. DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs
- c. IEEE/EIA 12207, "Information Technology – Software Life Cycle Processes"
- d. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)"

8.2 Acronyms.

C&A	Certification and Accreditation
CASE	Computer Aided Software Engineering
CCB	Configuration Control Board
CI	Configuration Item
CIO	Chief Information Officer
CM	Configuration Management
COE	Common Operating Environment
CONOPS	Concept of Operations
DII	Defense Information Infrastructure
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
IPPD	Integrated Product and Process Development
IT	Information Technology
IPT	Integrated Product Team
ITSEC	Information Technology Security
LAN	Local Area Network
OIS	Ordnance Information Systems
OSE	Open System Environment
QA	Quality Assurance
SCR	System Change Request
SEP	Software Engineering Process
SGML	Second Generation Markup Language
SSB	Strategy Steering Board
WAN	Wide Area Network

8.3 Definitions.

Best Practices – Management practices that avoid imposing government-unique requirements that may significantly increase industry compliance costs.

Common Operating Environment (COE) - The collection of standards, specifications, and guidelines, architecture definition, software infrastructure, reusable components, 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. .

Configuration Control - The systematic evaluation, coordination, approval or disapproval, and implementation of all approved changes in the configuration of an item, after the formal establishment of its configuration identification in approved configuration documentation.

Configuration Control Board (CCB) - A board composed of functional and technical representatives who recommend approval or disapproval of proposed engineering changes to a configuration item's current approved configuration documentation.

Configuration Item (CI) - An aggregation of hardware or software that satisfies an end use function and is designated for separate configuration management.

Configuration Management (CM) - As applied to configuration items, a discipline applying technical and administrative direction and surveillance over the life cycle of items to perform the following: identify and document the functional and physical characteristics of configuration items; control changes to configuration items and their related documentation; record and report information needed to manage configuration items effectively, including the status of proposed changes and implementation status of approved changes; and audit configuration items to verify conformance to specification, drawings, interface control documents, and other contract requirements.

Configuration Status Accounting (CSA) - The recording and reporting of information needed to manage a configuration effectively, including a listing of approved configuration documentation, the status of proposed changes to the configuration and the implementation status of approved changes.

Integrated Product and Process Development (IPPD) – The management technique that integrates all acquisition activities starting with requirements definition through development, fielding/deployment and operational support in order to optimize the design, business, and supportability processes.

Integrated Product Team (IPT) - Teams of technical and functional experts empowered to act in support of system development efforts. IPTs function in a spirit of teamwork with participants empowered and authorized, to the maximum extent possible, to make commitments for the organization or functional area they represent.

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.

Interfacing - The process of two components or systems exchanging information by first translating the information into an intermediate, agreed-upon format.

Interoperability - The ability of two or more systems or components to exchange and use information.

Open System - A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (a) to be ported with minimal changes across a wide range of systems, (b) to operate with other applications on local and remote systems, (c) to interact with users in a style that facilitates user portability, and (d) to enable users to increase processing power as their functional needs grow, without the need to re-write applications (i.e., scalability).

Portability - The degree to which system components may be transferred from one hardware or software environment to another.

Scalability - The ability of a system to increase (decrease) functionality, the amount of data which can be processed or stored, and responsiveness without the need to re-write applications through the addition (removal) of hardware and software components.

Appendix A -- Comment Summary

Customer	Comment	Action Taken
MARCORSYSCOM	Recommended Marine Corps CCB vote be identified as average of CMC(ASL) and MARCORSYSCOM (AM)	CONCUR – Change clarification made
	Recommended voting process be clearly delineated in the OIS CONOPS	CONCUR – Agree this should be included but added after the SSB and CCB have met and agreed upon the voting procedures. (i.e. – criteria for assigning priorities)
CINCLANTFLT	Add glossary	CONCUR – Added Section 8 – References, Acronyms and Definitions
CINCPACFLT	Need documentation for Help Desk processes and program fix prioritization	CONCUR – Advised this would be included in CM Plan
AOC Yorktown	No Comment	
WPNSTA Seal Beach	Same comments as CPF	
NSWC Crane	Change CCB voting member from NSWC to Warfare Center	CONCUR – Change made
Coast Guard	Add Coast Guard to SSB membership	CONCUR – Added
NALC	Change organizational relationship chart to show feedback arrows going out and in of User block	CONCUR – Change made to chart
SPECWARCOM	Add SPECWARCOM as a voting member of the SSB	CONCUR – Change made
	Add SPECWAR as an equal voting member on the CCB vice an element of Navy	NONCONCUR
	Rationale: Element of Special Operations Command	
OPNAV	Additions to OIS Program Objectives and Goals	CONCUR – Change made
	Recommendation to move SSB and CCB charter detailed information from body of the CONOPS	CONCUR – Moved charters to appendices

Table 1, Customer Comment Summary

OIS Project Response	Comment	Action Taken
CAIMS	No comment	
ROLMS	Add NAVSEA and Coast Guard to SSB membership SSB Membership – change NALC to NAVSUP SSB/CCB Membership – identify that primary member may designate an alternate Change “P” in IPT from product to process	CONCUR – Change made CONCUR – Changed to NAVSUP (NALC) CONCUR – Statement added to Charters DISAGREE – DOD Acquisition Deskbook identifies groups as Integrated PRODUCT Teams
RSSI	No comment	
ADIMS	Questions	Responses provided
DTTS	Don't envision joint requirements passing through the CCB for approval	

Table 2, OIS Project Response Comment Summary

Appendix B -- OIS SSB Charter

The Ordnance Information Systems (OIS) Strategic Steering Board (SSB) Charter is included, starting on the next page.

**ORDNANCE INFORMATION SYSTEMS
(OIS)
STRATEGIC STEERING BOARD
(SSB)**

CHARTER

1.0 PURPOSE AND SCOPE

The purpose of this charter is to establish and outline the membership, duties and responsibilities of the Ordnance Information Systems (OIS) Strategic Steering Board (SSB). The SSB is the senior management group that approves the OIS Program Strategic Plan and provides guidance to OIS project change control.

2.0 SSB MEMBERSHIP

The SSB consists of principal members and invited participants. Only principal members may vote on issues before the Board and each member has one vote.

2.1 Principal Members. Principal members shall include representatives from the following organizations:

- OPNAV (N411)
- CINCLANTFLT (N41)
- CINCPACFLT (N42)
- MARCORSSYSCOM (AM)
- CMC (ASL)
- NAVSEA
- Coast Guard
- NAVSPECWARCOM
- NAVSUP (NAVAMMOLOGCEN)

2.2 Invited Participants. Invited participants shall include representatives from:

- System Project Managers
- IPT Lead Managers

3.0 SSB ROLES AND RESPONSIBILITIES

The SSB will meet twice each fiscal year, or as required. The Ordnance CIO will coordinate SSB meetings, agenda, and related actions. Each SSB member shall be permanently assigned and have the authority to commit for the represented service, command or activity. It is recommended that each voting activity identify a primary and an alternate member.

3.1 SSB Roles. The SSB shall provide:

- Program guidance.
- OIS Program Strategic Plan Approval.
- OIS Program system(s) change concurrence and prioritization guidance.
- System(s) requirements approval.
- User community sponsorship.

3.2 SSB Responsibilities. The SSB is responsible for:

- Functional Representation/Program Guidance – Ensures that ordnance community requirements are satisfied by the OIS Program.
- Strategic Plan approval - Concurs with and recommends changes to the OIS Program Strategic Plan.
- Budget approval/direction of funding – Approves the allocation of funding based on the OIS Strategic Plan for strategic, tactical and operational changes.
- CCB Guidance – Provides the CCB with guidance.
- Strategic and tactical change concurrence - Concurs with strategic and tactical changes approved for implementation.

4.0 APPROVAL

Approved:

proposed signature is OPNAV N4

DATE

Appendix C -- OIS CCB Charter

The Ordnance Information Systems (OIS) Configuration Control Board (CCB) Charter is included, starting on the next page.

**ORDNANCE INFORMATION SYSTEMS
(OIS)
CONFIGURATION CONTROL BOARD
(CCB)**

CHARTER

1.0 PURPOSE AND SCOPE

The purpose of this charter is to establish and outline the membership, duties and responsibilities of the Ordnance Information Systems (OIS) Configuration Control Board (CCB). The CCB is the middle management group that reviews system changes from the user community, evaluates internal and external system(s) impacts, evaluates change resource requirements, and approves/disapproves requested changes as requirements.

2.0 CCB MEMBERSHIP

The CCB consists of principal members and invited participants. Only principal members may vote on issues before the Board and each member has one vote.

2.1 Principal Members. Principal members shall include representatives from the following organizations:

- Navy *
- Marine Corps **
- Coast Guard
- Ordnance CIO, Chair (non-voting)

Note:

* Navy's vote will be the average of one vote each from the following community representatives – CINCLANTFLT, CINCPACFLT, LANTORDCOM Yorktown, NAVWPNSTA Seal Beach, NAVSURFWARCEN, SPECWARCOM, and NAVAMMOLOGCEN).

** Marine Corps' vote will be the average of one vote each from CMC(ASL) and MARCORSYSCOM (AM).

2.2 Invited Participants. Invited participants shall include representatives from:

- Functional Users
- System Project Managers
- System developer representatives

3.0 CCB ROLES AND RESPONSIBILITIES

The CCB will meet twice each fiscal year, or as required. The Ordnance CIO will coordinate CCB meetings, agenda, and related actions. Each CCB member shall be permanently assigned and have the authority to commit for the represented service, command or activity. It is recommended that each voting activity identify a primary and an alternate member.

3.1 CCB Roles. The CCB shall provide:

- System change approval and prioritization.
- Functional user representation.
- Membership to the Integrated Product Team(s) (IPTs).

3.2 CCB Responsibilities. The CCB is responsible for:

- Guidance – Compliance with Ordnance CIO and Strategic Steering Board (SSB) direction and guidance.
- Change recommendations – Reviews user change requests, approves valid requests for changes as functional requirements, and manages system changes in accordance with the approved Configuration Management Plan.
- Initiative review – Reviews and approves management initiatives and business strategies, and keeps the user community informed of such initiatives.
- User community satisfaction – Conducts periodic user surveys to determine satisfaction with the system.

4.0 APPROVAL

Approved:

proposed signature is OPNAV N41 DATE