



DEPARTMENT OF THE NAVY
COMMANDER
NAVAL EDUCATION AND TRAINING COMMAND
250 DALLAS STREET
PENSACOLA, FLORIDA 32508-5220c

NETCINST 5200.3D
N6
03 JAN 2023

NETC INSTRUCTION 5200.3D

From: Commander, Naval Education and Training Command

Subj: INFORMATION TECHNOLOGY CONFIGURATION CONTROL

Ref: (a) NETC 2022 Information Technology System Portfolio
(b) NETCINST 5200.2D
(c) DoD Information Technology Portfolio Repository -
Department of the Navy Process Guidance (V1.0) of
5 December 2011
(d) DoD Instruction 8510.01 of 29 December 2020

Encl: (1) NETC Governance Minimum Sustainment Function
Definitions
(2) NETC Configuration Control Board Charter Template
(3) NETC Roles and Responsibilities of Program Managers
and Technical Managers

1. Purpose. To establish an authoritative framework for effective and innovative configuration compliance for Information Technology (IT) as it relates to Naval Education and Training Command (NETC) Training and Education (T&E). This policy establishes the Configuration Management (CM) governance, composition, function, responsibilities, and authority to implement a Configuration Control Board (CCB) governance model within NETC.

2. Cancellation. NETCINST 5200.3C.

3. Scope

a. This instruction only applies to the NETC portfolio legacy applications that have not been affected by the MyNavy Human Resources (HR) transformation effort. Per reference (a), the term "NETC portfolio legacy application" is defined as: NETC IT systems that are currently operating in a production environment, that may be planned for, but have not yet been, shutdown or consolidated as a result of the MyNavy HR transformation program. This instruction will remain in effect

until all NETC legacy applications have been transformed and shut down.

b. CM requires controls and audits the functional and physical characteristics of information systems, equipment, software, and other designated material items, such as:

(1) Management and administrative procedures so that the information manager can identify, control, and change hardware and software.

(2) Administrative processes, status accounting, and reports to reduce interface problems between different systems.

(3) Procedures to report problems, implement solutions, and control systems evolution.

c. Reference (b) provides the IT Governance for creating a framework which requires NETC to align business strategy and priorities with IT investments. The NETC Command Information Officer (CIO) is accountable to ensure compliance with higher authority mandates and to control changes affecting IT systems. A key part of managing change to any IT Program of Record (POR) is establishing and enforcing change control policies. This will minimize problems by identifying conflicting changes and ensure that stakeholders have access to the current approved configuration control work products.

d. Reference (c) requires PORs to have a designated Project Manager (PM) and Technical Manager (TM) who are registered in Department of Defense (DoD) Information Technology Portfolio Repository - Department of the Navy (DIPTR-DON). The designated PMs and TMs will establish and co-chair system CCBs. Enclosure (1) outlines NETC's minimum sustainment services and their definitions. Any request for IT services that does not fall under the above definition is deemed to be "Above Core" and must be submitted through a Change Request (CR) or similar documentation. Approved requirements and CRs will be passed to PM for review and adjudication prior to submission to the NETC CCBs for prioritization and planning.

4. Responsibilities

a. NETC N6 is designated as the NETC CIO and is accountable for the technical oversight and operation of all T&E PORs. NETC CIO will ensure the system will be compliant with current Cyber policies, funded for ongoing sustainment, and in compliance with appropriate Navy and Personnel, Manpower, and Training (PMT) data standards. NETC CIO will designate an IT Portfolio Manager (PfM) to serve as the IT configuration control authority for all formal work elements pertaining to all PORs managed under T&E IT Governance. The PfM will serve as the IT compliancy authority to all working elements of T&E IT Governance including the T&E Functional Review Board (FRB). The PfM will participate as needed with IT efforts being reviewed by NETC Functional Managers (FM) to provide the business process direction including: recommending alternate options, providing project analysis, business oversight, technical and system architecture, and IT resource management data that may affect current priority of approved functional requests. Additionally, new functional requests affecting multiple or undetermined CCBs will be routed to the PfM for adjudication. The PfM will work with the FMs and FRB as needed to support IT project management and acquisition needs as they arise. See Figure 1 for PMT IT Governance responsibilities. The PfM will additionally provide DoD Architecture Framework (AF) technical artifacts required for the DITPR-DON Annual Review, and architecture diagrams on new capability initiatives. The NETC Data Steward operates under the guidance of PfM, and identifies T&E IT Data Management needs across all CCBs. The NETC Data Steward is a non-voting member in all NETC CCBs.

b. FMs are assigned by the NETC Division Directors (N-Codes). They are responsible for their applicable business capability and business process area assessment and current governing business policies. Per reference (b), FMs will ensure IT functional requirements address capability gaps and are clear, concise, and actionable. They are also responsible for functional prioritization within their area of responsibility and for initiation of those requests to the appropriate CCB area.

c. NETC N6 will maintain a Configuration Management Plan (CMP). The CMP defines the scope, responsibilities, and

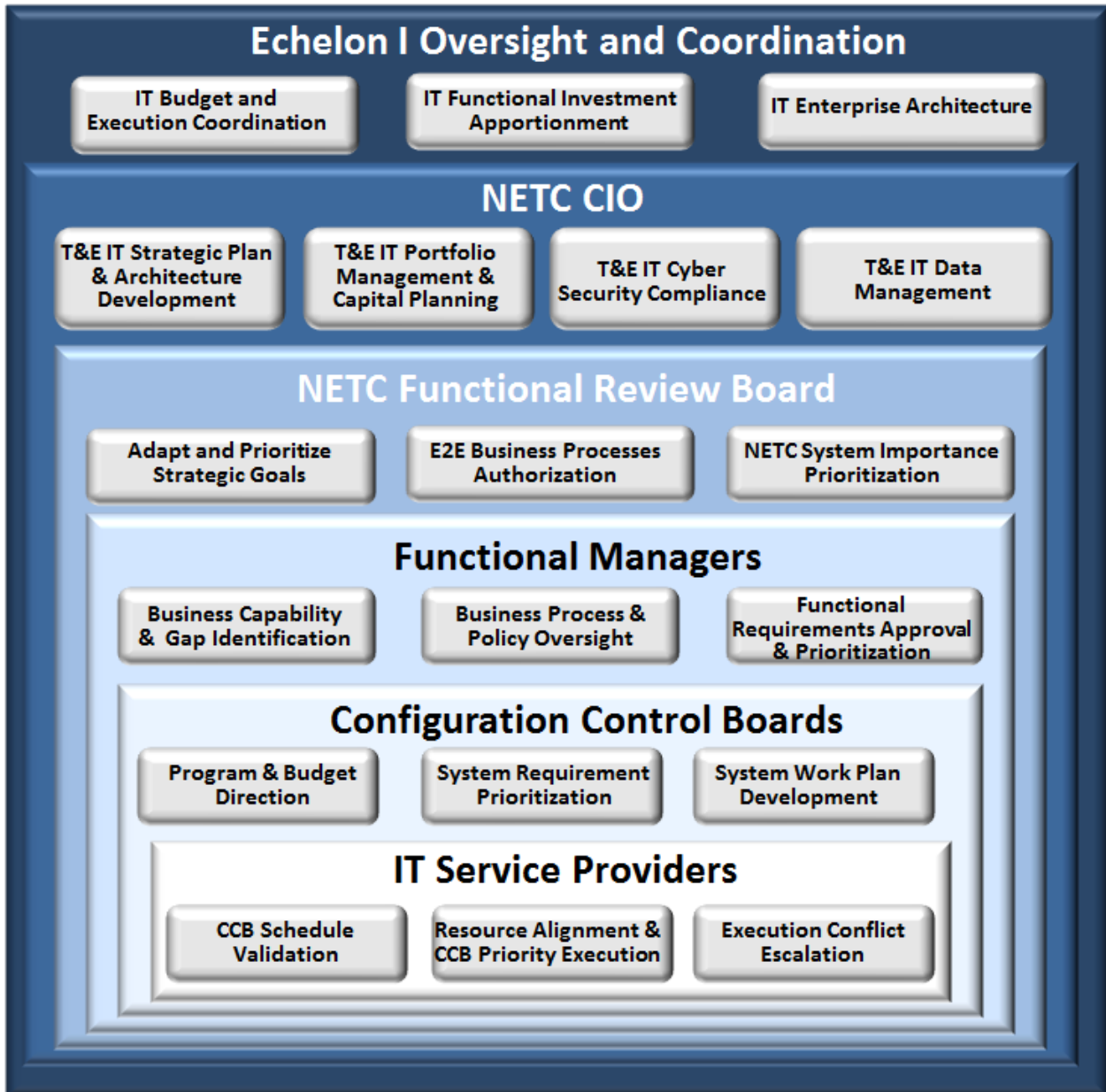


Figure 1. PMT IT Governance Responsibilities

methodology for CM of the organizations including: networks, security products, and both software and hardware. The CMP is intended as a management tool to ensure effective CM planning, implementation, configuration control, and status reporting. This plan delineates policy, technical and administrative direction, procedures, and responsibilities when configuration items are affected. Configurations are controlled through a

series of processes that begin with a program decision to develop and review a proposed change and to ensure that all changes to NETC IT applications occur within an identifiable, controlled environment and end with an approved, tested, and installed change. NETC N6 is also the primary technical liaison and Point of Contact (POC) for configuration coordination of external service providers such as Navy Enterprise Data Center New Orleans and Naval Air Warfare Center Training Systems Division. They will also designate an Information Assurance Manager or Information Assurance Officer to represent Information Assurance issues which pertain to a specific IT System and to participate in security and compliance related CCB decisions.

d. NETC CCBs are authorized to act on behalf of the NETC CIO to manage the configuration control process, provide governance and direction of NETC PORs, and convene assigned POR CCB as needed. The PM, as designated in the DITPR-DON, will establish a CCB Charter for each POR using enclosure (2) as a template. The CCB charter must describe the composition of the board, including roles and responsibilities, associated functions and authority of CCB members, and planned convening frequency. CCBs have directed authority to mitigate and prioritize critical configuration baseline issues which exclusively pertain to the IT application. CCBs will be responsible for maintaining visibility of the status of project requests to manage the workload associated with CR submissions. CCBs will execute IT Application work plans including shared service and sustainment. The CCB is responsible for reviewing completed CR packages for adjudication of availability of resources. CCBs will also recommend convening User Working Groups (UWG), as needed, to ensure subject matter expert input for specific issues. The PM will establish UWGs, as needed, to initiate required decision support documentation to invoke change requests, business process improvements, and submit recommendations for NETC policy changes. CCB co-chairs will partner together to create schedule meeting date(s) for the CCB which will convene at least quarterly each calendar year. Enclosure (3) defines the PM and TM roles and responsibilities assigned to each IT POR.

(1) PMs will submit the written charter for the CCB to the NETC CIO for approval. Reference (c), which governs the management of IT systems within the DON, and reference (d),

which provides a risk framework for IT systems, require that all IT systems and PORs have designated PMs. The co-chairs of the CCB are responsible for providing a consolidated work plan for each fiscal year in the timeframe communicated by the annual IT Planning Calendar, prioritization of all system requirements from all sources, sustainment budget reviews, and potential impacts of system development projects. PMs are accountable for fiscal planning and programming, and will coordinate with the appropriate stakeholders concerning any change requests requiring resources to support discretionary, above core, or minimum sustainment thresholds during the configuration control process. Each PM will establish an effective line of communications to the responsible FM who is assigned those functional areas which the subject IT system directly supports. PMs and TMs are the primary Technical Advisors for the Contracting Officer Representatives on task orders funded by their applications. PMs and TMs will maintain an accurate understanding of the Total Cost of Ownership for their system, track their sustainment baseline, using budget and expense visibility information from official Navy systems.

(2) TMs share certain responsibilities with PMs as indicated above, and will provide overall program direction to technical teams and serve as the escalation POC between the PM, CCB, and responsible IT service provider. TMs identify delivery capacity gaps and recommend trade-off analysis of alternatives to the CCB and the PM, including both minimum sustainment and new functional capability as assigned.

e. IT Service Providers are responsible for aligning resource capacity to CCB-defined priorities and for identification of shared service resources conflicts. Where shared service conflicts are identified, IT Service Providers are required to review internal actions that may resolve the conflict and recommend mitigation to affected CCB owners.

5. Action

a. Each NETC POR will have an authoritative CCB for the purpose of prioritizing critical configuration technical requirements, operational and systems migration and integration functional requirements, and any and all development issues which impact the IT application as part of the IT Governance Process.

b. Each FM will assign PMs to the NETC CIO for the appropriate CCBs.

c. NETC N6 will designate a TM for each POR, who will be assigned to the respective CCB.

6. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned per the records disposition schedules located on the DON Assistant for Administration, Directives and Records Management Division portal page at <https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/>.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact the local records manager.

7. Review and Effective Date. Per Office of the Chief of Naval Operations Instruction (OPNAVINST) 5215.17A, NETC will review this instruction annually around the anniversary of its issuance date to ensure applicability, currency, and consistency with Federal, Department of Defense, Secretary of the Navy, and Navy policy and statutory authority using OPNAV 5215/40 (Review of Instruction). This instruction will be in effect for 10 years, unless revised or cancelled in the interim, and will be reissued by the 10-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.


C. COLLINS, JR.
Chief of Staff

Releasability and distribution:

This instruction is cleared for public release and is available electronically on the NETC Public web site (www.netc.navy.mil) or by e-mail at netc-directives@us.navy.mil.

NAVAL EDUCATION AND TRAINING COMMAND GOVERNANCE MINIMUM
SUSTAINMENT FUNCTION DEFINITIONS

Minimum Sustainment - includes the following:

Core Services. Core services are those components required to keep a system running so that it is operationally available. This includes required hardware license and software license maintenance, security, planning and management, production support, and Configuration Management (CM) activities. It also includes the operations environment (e.g., Space and Naval Warfare Systems Center Atlantic New Orleans, Naval Information Center Pacific, Continuity of Operations Planning, and Defense Information Systems Agency) and database administration functions to maintain systems operations and availability. Core Services only provide support for system breakage and emergency fixes to keep the system operational. It does not provide support for system Change Requests (CRs) for maintenance or enhancements and includes the following:

- Computer Operations
- Software License Maintenance
- Hardware License Maintenance
- Database Administration
- Security
- Planning and Management
- Production Support
- CM
- Mandatory CRs on a case-by-case basis within funded ceiling that are required due to:
 - Legislative changes
 - Naval Education and Training Command Manpower policy directed changes by Department of Defense, Chief of Naval Operations, or Chief of Naval Personnel
 - Critical interface changes

NOTE: Any request for Information Technology services that does not fall under the above definition is deemed to be "Above Core" and must be submitted through a CR or similar documentation.

NAVAL EDUCATION AND TRAINING COMMAND CONFIGURATION
CONTROL BOARD CHARTER TEMPLATE

1. Configuration Control Board Purpose. The purpose of the Configuration Control Board (CCB) is to ensure that programmatic changes (i.e., consideration of proposed cost and schedule changes) and related technical changes to information systems are processed in a visible and traceable manner. The CCB is the forum in which: (1) participants get together to discuss specified work assignments which need to be completed; (2) responsible agents are assigned for performing agreed-upon work; and (3) decisions and assigned actions are recorded as they are completed. This includes providing technical support during development of decision support documentation such as Change Requests, System Functionality Assessments, Analysis of Alternatives, Independent Cost Estimates, etc.

2. CCB Chairpersons. The CCB is co-chaired by the appointed Project Manager (PM) and Technical Manager (TM). Together they will manage the meeting in such a manner that input and discussion are encouraged from all attendees. Product and programmatic decision authority rests with the PM and is made a matter of record in the meeting documentation.

3. CCB Membership. The CCB will be comprised of the following representatives:

- PM - (To Be Determined (TBD) - identify representative(s) by name and title)
- TM - (TBD - identify representative(s) by name and title)
- Data Steward (Advisory)
- Other Assigned Members and UWGs (as designated by the CCB)

4. CCB Activities. The CCB will meet on a predefined schedule: (TBD - specify frequency of CCB meetings, also specify any requirements for meeting notification, quorum of attendees, etc.). The CCB will perform the following activities: (TBD - the following activities are presented as examples of the CCB activities to be included. This list should not be considered complete until it has been approved by the Information Technology organizations participating in the CCB.)

- Reviewing and managing proposed changes to the system architecture
- Reviewing and managing cross-organizational application issues
- Reviewing and managing the Configuration Management process
- Recording CCB minutes, reviewing, approving, and, if necessary, recording changes to CCB minutes from the previous CCB meeting

5. CCB Meeting Documentation. The following information will be recorded for each CCB meeting: (TBD - the following items are presented as examples of the information to be included in the CCB minutes. This list should not be considered complete until it has been approved by the IT organizations participating in the CCB.)

- Meeting date, time, and duration
- List of attendees and their organizations
- Items discussed
- Existing and new action items
- Decisions made

NAVAL EDUCATION AND TRAINING COMMAND ROLES AND RESPONSIBILITIES
OF PROGRAM MANAGERS AND TECHNICAL MANAGERS

1. Functional Managers (FMs) are responsible for business process effectiveness and roadmap for system capability changes, including establishing functional priorities within their functional area.

2. Project Managers (PMs) are the functional subject matter experts for an assigned Information Technology (IT) system or systems and therefore, serve as the focal Point Of Contact (POC) for all required Program Of Record (POR) information. PMs will report the system annual work plans, project priority recommendations, budget reviews, and potential production project impacts to the Naval Education and Training Command (NETC) Functional Review Board (FRB). The PM identifies and defines system functional requirements. Additionally, the PM plans, organizes, and coordinates the development, production, procurement, and financial management processes for assigned programs and systems to include the approval and certification of Department of Defense (DoD) funds and annual review data call specified in the National Defense Authorization Act for Fiscal Year 2005. Other PM responsibilities include, but are not limited to:

a. Entry point for all new requirements within their program area, and responsible for ensuring functional requirements are clear, verifiable, and actionable prior to formal acceptance of the change request. PMs are accountable for CCB priorities and review and analyze functional requirements for completeness, clarity, and actionability. The PM will resolve deficiencies with the submitter as appropriate to define the functions or internal processes within a system or its component.

b. Provide the DoD Architecture Framework (DODAF) operational artifacts required for the Integrated Business Framework Data Alignment Portal Annual Review (i.e., Capabilities Views (CV), Operational Views).

c. Ensure compliance with the Business Enterprise Architecture and Department Of the Navy (DON) Enterprise Architecture.

d. Ensure all data in the DoD Information Technology Portfolio Repository-DON (DODITP-DON) is valid, current, and illustrates an accurate representation of the state of the system.

e. Build an Annual Work Plan for the associated IT system. The plan will outline all functional changes to the configuration baseline to ensure requirements are properly identified, recorded, evaluated, and approved or disapproved, incorporated, and verified along an aggressive timeline.

f. Maintain oversight of all funding requirements, expenditures, and visibility of all costs associated with the system's fiscal line of accounting based on a sustainment baseline they maintain. PMs are the system requirements authority for Program Objective Memorandum, mid- and end-of-year adjustments and Defense Business System Certification, and visibility of the end-to-end budget.

g. Coordinate semiannual Program Reviews for NETC leadership to assess investment plans, portfolio costs, and planned Level of Effort (LOE).

h. Ensure the IT system is able to meet required business capability and performance.

i. Co-chair CCBs along with the TMs.

3. TMs are responsible for all system related program resources (i.e., hardware, software, connectivity) and the performance of all resources to support IT systems including minimum Sustainment and Shared Services, Cyber Security, Administrative, CM, and Operations and Infrastructure. As the CCB co-chair, TM responsibilities include, but are not limited to, the following:

a. Act as technical focal POC between the functional PMs and the service providers, both internal and external to NETC.

b. Support the PM in ensuring new functional requirements are sufficient to conduct technical requirements analysis, and TMs are responsible for determination of requirement impact, estimations for implementation, and technical specifications. Technical specifications define how information technologies are leveraged to automate the delivery of capabilities and compliances in order to satisfy user functional requirements.

c. Ensure that computer systems function properly and are up to date and protected with appropriate security.

d. Provide DoDAF technical artifacts required for the DITPR-DON Annual Review (i.e., CVs, System Views, and Services Views).

e. Provide CM oversight by ensuring changes are carefully evaluated before being applied and are made in a timely, effective, and consistent fashion.

f. Provide oversight over all minimum sustainment funding requirements and expenditures. TMs will work with shared service manager and leads to ensure work plans reflect minimum sustainment capacity LOE to support shared service requirements.

g. Identify delivery capacity gaps and recommend trade-off analysis of alternatives to the CCB and the functional PM, including both minimum sustainment and new functional capability as assigned.

h. Provide overall program direction to technical teams and serve as the escalation POC between the functional PM, CCB, and service provider.

i. Coordinate quarterly in-process reviews of assigned IT system for NETC leadership to assess work plans, schedules, risks, and performance.

j. Assist the PM in developing an Annual Work Plan for the associated IT system. The plan will outline all technical changes to the configuration baseline to ensure specifications and compliance requirements are properly identified, recorded, evaluated, approved or disapproved, incorporated, and verified along an aggressive timeline.

k. Assist PM in preparing for the Quarterly Program and Annual Investment Reviews.