DCMA Manual 4401-05

Information Technology Change/Configuration Management (CM-1)

==========

Office of Primary Responsibility:	**Information Technology Management Capability**
Effective:	December 20, 2021
Releasability:	Cleared for public release
New Issuance	
Implements:	DCMA Instruction 4401, "Information Technology Management," January 20, 2020
Internal Control:	Process flow and key controls are located on the Resource Page
Labor Codes:	Located on the Resource Page
Resource Page Link:	https://360.intranet.dcma.mil/Sites/Policy/ITM/SitePages/4401-05r.aspx
Approved by:	David G. Bassett, LTG, USA, Director

Purpose: This issuance, in accordance with the authority in DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," DoD Directive 8440.01, "DoD Information Technology Service Management":

- Implements policy established in DCMA Instruction 4401
- Standardizes methods and procedures for efficient and prompt handling of technical changes to the Information Technology environment
- Minimizes the impact of change-related incidents to service quality
- Improves day-to-day operations of the organization

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to all DCMA activities unless higher-level regulations, policy, guidance, or agreements take precedence.

1.2. POLICY. It is DCMA policy to:

a. Have a formal, repeatable process that minimizes risk to be used when introducing change to the DCMA-Information Technology (IT) environments. The change management (ChM) process ensures that all changes are assessed, approved, implemented, and reviewed in a controlled manner. ChM will ensure that any modification to the DCMA IT environment establishes an orderly and effective procedure for tracking the submission, coordination, review, evaluation, categorization, and approval for release of all changes to an IT service or IT service component.

b. Execute this Manual in a safe, efficient, effective, and ethical manner.

SECTION 2: RESPONSIBILITIES

2.1. DEPUTY CHIEF INFORMATION OFFICER (DCIO). The DCIO will:

a. Be the process owner for ChM.

b. Establish and charter the DCMA-IT Change Advisory Board (CAB).

c. Assign CAB membership and responsibilities.

d. Outline the CAB's authority, membership, responsibilities, and procedures as they relate to the governance (GOV) of ChM and configuration management (CfM) within DCMA.

2.2. IT-SENIOR LEADERSHIP TEAM (IT-SLT) MEMBER. The IT-SLT member will:

a. Designate CAB members to represent their respective directorates.

b. Designate Configuration Item (CI) owners within their respective directorates.

c. Be a member of the Emergency CAB (ECAB) and authorize emergency changes for implementation.

2.3. CHANGE REQUESTER. The Change Requester will:

a. Identify the requirement for a change.

b. Complete and submit a Request For Change (RFC) (See Section 6).

c. Provide additional information about the RFC and attend CAB meetings, if invited.

d. Coordinate and assign implementation tasks required to complete the RFC.

e. Review the change when requested, and specifically before closure.

2.4. CHANGE IMPLEMENTER. The Change Implementer will:

a. Implement changes.

b. Update RFC documentation with required information.

2.5. CHANGE MANAGER. The Change Manager will:

a. Act as a facilitator, responsible for the overall ChM process.

b. Authorize or reject normal changes and approve or reject emergency changes.

c. Coordinate and conduct meetings with CAB to discuss higher risk changes.

d. Ensure that all the activities designed to implement the change are as per the standards.

e. Prepare Change Summary Sheet that summarizes all RFCs. This sheet helps the CAB understand and evaluate proposed changes.

2.6. CHANGE AUTHORITY. The Change Authority will:

a. Review specific categories of RFC.

b. Formally approve changes at agreed points in the change lifecycle.

c. Participate in the change review before changes are closed.

d. Attend CAB meetings to discuss and review changes when required.

2.7. CAB CHAIR. The CAB Chair will:

a. Decide who will attend CAB meetings and notify them accordingly.

b. Plan, schedule, manage, and chair CAB meetings.

c. Select RFCs for review at CAB meetings, based on the change policy.

d. Circulate RFCs in advance of CAB meetings to allow prior consideration.

e. Convene ECAB meetings for consideration of emergency changes, if required.

f. Approve emergency changes that have been authorized by the ECAB.

g. Select successful and failed changes for review at CAB meetings.

h. Prepare an external RFC when the proposed change will cause a significant impact to the DCMA-IT architecture or operations.

i. Prepare an external RFC for approval of modifications, option year execution, or new IT Service Contracts.

j. Prepare an external RFC and submit IT purchase request(s) to request approval of hardware and software purchases.

2.8. CAB MEMBER. The CAB Member will:

a. Attend scheduled meetings or designate a proxy who is empowered to make decisions on their behalf in the area they represent.

b. Make recommendations for implementation, further analysis, deferment, or cancellation of RFCs.

c. Designate changes that meet the 4th Estate Network Optimization (4ENO) significant or major threshold.

2.9. SECRETARIAT. The Secretariat will:

a. Serve as the official record keeper for CAB documentation by overseeing the maintenance and preservation of supporting and historical data that constitute as official records.

b. Post and maintain final documentation on the DCMA Change Management 360 site for dissemination and collection of CAB information and data.

c. Publish meeting agenda.

d. Prepare and distribute packages including System Change Requests, RFCs, and action items to be discussed at least 48 hours prior to the scheduled meeting with direction from the Chair.

e. Track the status of System Change Requests, RFCs, and action items.

f. Plan and schedule meetings, record attendance, develop meeting minutes, distribute agenda items, and document tasks and actions.

g. Obtain Chair's and CAB Members' signatures (or e-mail approvals, if applicable) on all required meeting decisions.

h. Follow any additional guidance per the CAB Chair.

2.10. 4ENO CAB CHAIR. The 4ENO CAB Chair will:

a. Manage the review of major and significant change requests submitted by 4th Estate organizations.

b. Request additional information, if required.

c. Provide a response within 2 to 3 business days.

2.11. CfM PROCESS OWNER. The CfM Process Owner will:

a. Ensure the required processes and procedures to manage CIs in all IT environments are established.

b. Ensure that the process is performed according to the agreed and documented standard.

c. Sponsor, develop metrics, and manage the CfM process in accordance with policy and industry best practices.

d. Periodically audit the process to ensure compliance to policy and standards.

e. Communicate process information or changes, as appropriate, to ensure awareness.

f. Ensure process technicians understand their role in the process and have the required knowledge, technical, and business understanding to deliver the process.

g. Review opportunities for process enhancements and for improving the efficiency and effectiveness of the process.

2.12. CfM PROCESS MANAGER. The CfM Process Manager will:

a. Be the policy guardian for the CfM process.

b. Be accountable to the organization for stewardship of fixed assets that are under the control of IT.

c. Manage resources assigned to the process.

d. Work with the process owner to plan and coordinate all process activities to include improvements to the process.

e. Monitor and report on process performance and identify process improvement opportunities.

f. Define the service assets that will be treated as CIs.

g. Be responsible for the day-to-day operations of the process.

h. Coordinate interfaces between CfM and other processes, especially ChM, release and deployment management, and knowledge management.

2.13. CONFIGURATION ANALYST. The Configuration Analyst will:

a. Support and take direction from the Configuration Manager as the primary representative for a specific CI category.

b. Contribute to defining the structure of the CfM system, including CI types, naming conventions, required and optional attributes and relationships.

c. Record, maintain, and report on CIs (within scope) in the Configuration Management Database (CMDB).

d. Train staff in configuration management principles, processes and procedures.

e. Perform configuration audits.

2.14. CI OWNER. The CI Owner will:

a. Serve as the primary point of contact for the CI.

b. Be accountable for ensuring the CI is maintained in accordance with Information Assurance policies and processes.

c. Update the CI's entry in the CMDB to reflect updated and accurate data.

2.15. CONFIGURATION LIBRARIAN. The Configuration Librarian will:

a. Be the custodian of service assets that are registered in the CfM system.

b. Periodically audit the CMDB.

c. Control the receipt, identification, storage, and withdrawal of all supported CIs.

d. Maintain and provide status information on CIs as appropriate.

e. Archive superseded CIs and assist in conducting configuration audits.

f. Identify, record, store, and distribute issues relating to CfM.

SECTION 3: INFORMATION TECHNOLOGY CHANGE MANAGEMENT

3.1. IT ChM GENERAL PROCEDURES. ChM ensures that any modification to the IT environment, whether it involves an addition, modification, or deletion of a service or service component, is in line with the overall mission strategy. These are the general procedures for implementation of changes:

a. Changes to CIs will be tracked in the Service Management System.

b. Changes will be managed in accordance with the ChM process.

c. Changes will be associated with the CI being changed for historical data and planning purposes.

d. New CIs that are created as a result of changes will be recorded in the CMDB in accordance with the CfM Process.

e. The owner of CIs being changed in the production environment will be accountable for ensuring emergency changes are applied to development and test environments.

f. IT Directors have the authority to authorize emergency changes, however, they require CAB Chair approval and assignment prior to implementation.

g. IT staff will record time spent implementing changes in the ChM system.

h. The IT-SLT will designate and approve members through appointment letters.

i. Emergency changes will be associated with a problem record that is managed in accordance with the Problem Management process.

j. Any change that alters the basic security structure or security architecture requires Cybersecurity validation from the subject matter expert and a review of its effects to an issued accreditation.

k. The Change Authority, that authorized the change, must review any and all failed or partially failed changes.

l. Changes affecting 50 to 79 percent of the DCMA enterprise and/or IT operations will be designated as significant.

m. Changes affecting greater than 80 percent of the DCMA enterprise and/or IT operations will be designated as major.

n. Significant and major changes must be submitted to the 4ENO CAB for approval prior to implementation.

o. Report modifications, option year execution, or new IT service contracts to the 4ENO CAB.

p. Report hardware and software purchases to the 4ENO CAB.

SECTION 4: CHANGE CATEGORIES

4.1. CHANGE CATEGORY. Change Category definitions are:

a. Emergency. A change request to repair a failure or imminent failure. This RFC is associated with a critical priority (i.e., severe impact and urgency) problem ticket that affects production, causes outages or significant degradation in business, or is accompanied by sufficient business justification. In most cases, this request is executed with limited documentation and is outside the standard change schedule time. It will be reviewed later to ensure that latent errors were not introduced to production.

b. Standard (pre-approved). A pre-approved change is low-risk and adheres to an approved, typically well-tested procedure or work instruction. It is relatively common and is the accepted solution for a specific requirement. It will be documented on a master list of approved standard changes.

c. Normal. If a change is neither standard nor emergency, then it is categorized as normal. Therefore, the RFC is not a repeatable, previously documented change (standard), is not the result of a critical priority problem management ticket and is not accompanied by sufficient justification (emergency).

4.2. CHANGE IMPACT. Impact is often directly related to the extent to which the service has degraded from agreed upon service levels. Impact can be measured by the number of people affected, the criticality of the system affected, and the disruption to mission as a result of the service degradation or disruption. Impact classification definitions are:

a. Low. Insignificant impact on mission operations.

b. Medium. Impact to an administrative or support area of the Agency.

c. High. A major disruption impacting critical mission functionality or a significant number of personnel.

4.3. CHANGE URGENCY. Specifies the value that defines the importance of the change request, and reflects how quickly a change must be implemented, or the time available to reduce the impact of the change on the business. Urgency classification definitions are:

a. Low. The change addresses a minor or limited impact that affects a partial area of the Agency.

b. Medium. The change addresses a moderate or large impact to key areas of the Agency.

c. High. The change addresses a critical or widespread impact to the Agency or compromised information security.

4.4. CHANGE RISK. Risk defines the potential disruption of business operations associated with a given change request. A risk is measured by the probability of a threat or the consequences to the IT service if that failure occurs. The Change Risk Coding Matrix is located on the Resource Page. Risk definitions are:

a. None. The change has no significant potential for disruption and may impact less than 10 percent of clients.

b. Low. The change may interrupt or delay mission operations with little impact on commitments:

- Requires no work outage
- Affects only one noncritical application or system
- Affects 10 to 25 percent of clients (a limited number)
- Involves changes that are made during nonproduction hours

c. Medium. The change may interrupt or delay mission operations, which affects commitments:

- Requires a limited outage
- Affects a few applications or one mission-critical application IT ChM process
- Requires a business application redesign or enhancement
- Affects than 25 to 50 percent of clients (use impact for guidance)

d. High. The change may severely impact Agency operations:

- Requires a widespread outage
- Affects multiple business-critical applications
- Requires a new business application or a major redesign
- Affects more than 50 percent of clients (use impact for guidance)

4.5. CHANGE PRIORITY. Priority reflects the overall prioritization of the change based on impact and urgency. Higher priority changes will be given preference for building, testing, and implementation resources. The Change Priority Coding Matrix is located on the Resource page.

a. Low. A change is justified and necessary but can wait until the next scheduled release or upgrade.

b. Medium. There is no severe impact, but change cannot be deferred until the next scheduled release or upgrade.

c. High. Severely affecting some key users or impacting a large number of users.

d. Critical. Causing significant mission impact or ability to deliver key services. Immediate action required.

SECTION 5: CHANGE ADVISORY BOARD OPERATIONS

5.1. CAB GUIDING PRINCIPLES. CAB guiding principles include:

a. The CAB is comprised of representatives and alternates from IT functional areas and appropriate non-IT functional areas. These representatives are considered the subject matter experts. CAB member appointment letters are maintained on the Information Technology Service Management (ITSM) site. The Change Manager and CAB decide whether more or fewer groups are represented.

b. CAB members, representatives or alternates will communicate to their respective IT functional areas on a timely basis, and provide follow-up activities.

c. The Change Manager/CAB Chair will schedule regular meetings of the CAB to be attended by the designated representatives and stakeholders.

d. Participating members and appointed representatives are required to attend meetings to represent their interests but may defer to their appointed alternate when attendance is not possible.

e. The Change Requester may present information on changes at the CAB meeting.

f. If the owner or a designated substitute does not represent a change that requires more information at a CAB meeting, then the change may be deferred or rejected.

g. The CAB can postpone a change if it is determined that the change does not follow change policy or is logistically unworkable. The Change Manager informs the owner.

h. The CAB will follow a defined agenda to maintain consistency and transparency and ensure that the necessary matters are covered.

5.2. CAB MEETING. The CAB meetings are formal and controlled. The Chair convenes the meeting and follows the steps below:

a. The meeting will begin by recording attendance and by adhering to the IT ChM process.

b. Review any failed changes or change management circumventions, as these are likely to have consequences.

c. Review and close action items from the previous meeting minutes.

d. Discuss any problems resulting from old changes. If necessary, set up a Post Implementation Review meeting to deal with issues.

e. Review any category of changes that will be categorized as "business as usual" to avoid repeated examination by the CAB (Creation of Standard Changes).

f. Review the list of RFCs and agree on the order in which to evaluate them.

g. Examine RFCs for risks of collisions or interference, due to proximity of simultaneous or similar changes:

(1) Group changes by category (software, hardware, server, etc.).

(2) Examine proposed change dates for collisions and or potentially incompatible activities.

h. Identify any RFCs that are actually projects, not tasks. Projects, unlike tasks, have multiple steps that are dependent upon each other. Verify that a project manager has been assigned for planning, coordination, and execution. If the project dependencies have not been adequately evaluated, it is entirely appropriate to reject the RFC and request that new RFCs be submitted for each of the tasks.

i. Evaluate and authorize the RFC.

j. Schedule the approved changes on the Forward Schedule of Change and assign a Change Implementer.

k. Send rejected RFCs back to the respective Change Requester for further clarification or response to CAB comments.

l. The CAB meeting will be restricted to evaluating and approving RFCs, and will not get bogged down in process issues. Instead, dock these issues to be handled in a separate meeting. The goal is to keep the change management meetings focused on accomplishing the task at hand: review and approval of change requests.

SECTION 6: CHANGE REQUEST SUBMISSION PROCEDURES

6.1. CHANGE SUBMISSION AND APPROVAL LEAD TIMES. This section defines the lead time required for change request submission. The expectation is that the Change Requester will submit changes with the defined lead time to ensure adequate time for the review of a change request and subsequent approval. Lead times will ensure sufficient time for CAB members to review the documentation prior to the meeting and determine whether to approve, reject, or request additional work. For example, changes being reviewed and assigned during the weekly Deployment Readiness Review for implementation over the weekend must be submitted at least a week prior. Lead time requirements center on a change being submitted in time for the CAB weekly cycle. The "Lead Times Based on Change Type" is located on the Resource Page.

6.2. HOW TO DOCUMENT A RFC. Documentation creates a record that will retain the complete history of a given change. Different types of RFCs will require different degrees of data documentation specified by the artifact matrix. However, there is a baseline of data required to submit a RFC and additional information required for CAB review. The "How To Document a RFC" example is located on the Resource Page. Baseline RFC record data fields include:

a. Requester. The Requester field is required. The email address and phone number will be populated from Active Directory.

b. Summary. This field is required for submission as defined in the process document.

c. Description. This field is required for CAB review.

1. Provides a reason to perform a change.

2. Details the negative impact to the business if a change is not performed.

d. Change Type. This field is required for submission as defined in the process document.

e. Category, Impact, Urgency, Priority, and Risk. These fields are required for submission as defined in the process document.

f. Impacted Business Resources (CIs). This field is required for CAB review and will provide a list of items to the remote group for input into the inventory or CMDB.

g. Impacted Business Services. This field is required for CAB review and will provide a list of services being impacted by this change.

h. Due Date. This field is required for submission as defined in the process document.

i. Required Supporting Documents. This area includes any documentation that is determined to be a requirement for moving forward to the approval stage.

j. Planned Implementation Information. Includes planned implementation date, planned completion date, duration, and level of effort.

6.3. RFC DOCUMENTATION PRINCIPLES. All changes have a business justification, documented resource, and a defined feasible technical solution.

a. Unless previously exempted, any change to the IT environments requires a change request in the change system.

b. To the maximum extent possible, Change Implementers will use template forms or data entry screens and workflows to ensure consistency during the execution of standard and repetitive changes.

c. Use established change priorities as guidelines in the decision. The Change Manager is the neutral arbiter for assignment review. If an agreement cannot be reached with the Change Manager, then appeal to the next-most-senior level of management.

6.4. NORMAL ChM PROCESS. If a change is neither standard nor emergency, then it is categorized as normal. Therefore, the RFC is not a repeatable, previously documented change (standard), is not the result of a critical priority problem management ticket and is not accompanied by sufficient justification (emergency). The "Normal ChM Process Flow" is located on the Resource Page.

a. Create RFC. The Change Requester documents and submits the RFC.

b. Review RFC. The Change Manager reviews the RFC for completeness and filters out any requests that are incomplete or duplicates that have been accepted, rejected, or still under consideration.

c. Assess and Approve RFC. The RFC is presented to the CAB for review and the change is approved or rejected. Approved changes are scheduled appropriately and added to the overall change schedule.

d. Implement Change. The Change Implementer deploys the change.

e. Validate Change. The Change Requester validates the implementation and submits it for review and closure.

f. Review and Close. The Change Manager closes the RFC after review and verification that activities and tasks have been completed.

6.5. EMERGENCY ChM PROCESS. A change request to repair a failure or imminent failure. This RFC is associated with a critical priority (i.e., severe impact and urgency) problem ticket that affects production, causes outages or significant degradation in business, or is accompanied by sufficient business justification. In most cases, this request is executed with limited documentation and is outside the standard change schedule time. It will be reviewed

later to ensure that latent errors were not introduced to production. The "Emergency ChM Process Flow" is located on the Resource Page.

a. Create RFC. The Change Requester documents the emergency and submits the RFC or performs the change if the issue has created a significant impact to DCMA operations. A RFC will be submitted as a follow-up within 24 hours.

b. Assess and Authorize RFC. An IT-SLT member reviews the RFC for urgency, risk, and impact to DCMA. The IT-SLT member authorizes it if it meets the emergency threshold.

c. Assess and Approve RFC. The Change Manager reviews the RFC for urgency, risk, and impact to DCMA operations. The Change Manager approves it if it meets the emergency threshold.

d. Implement Change. The Change Implementer deploys the change.

e. Validate Change. The Change Requester validates the implementation and submits it for review and closure.

f. Review and Close. The Change Manager closes the RFC after review and verification that activities and tasks have been completed.

6.6. STANDARD ChM PROCESS. A pre-approved change that is low-risk and adheres to an approved, typically well-tested procedure or work instruction. It is relatively common and is the accepted solution for a specific requirement. It will be documented on a master list of approved standard changes. The "Standard ChM Process Flow" is located on the Resource Page.

a. Create RFC. The Change Requester documents and submits the RFC.

b. Review and Approve RFC. The RFC is presented to the Change Authority for review and the change is approved or rejected. Approved changes are scheduled appropriately and added to the overall change schedule.

c. Implement Change. The Change Implementer deploys the change.

d. Validate Change. The Change Requester validates the implementation and submits it for review and closure.

e. Review and Close. The Change Manager closes the RFC after review and verification that activities and tasks have been completed.

6.7. SIGNIFICANT IMPACT ChM PROCESS. These changes follow the Normal ChM process, but require approval by the 4ENO CAB for changes affecting greater than 50 percent of the DCMA enterprise and/or IT operations. These significant and major changes must be submitted to the 4ENO CAB for approval prior to implementation. The "Significant Impact ChM Process Flow" is located on the Resource Page.

a. Create RFC. The Change Requester documents and submits the RFC.

b. Review RFC. The Change Manager reviews the RFC for completeness and filters out any requests that are incomplete or duplicates that have been accepted, rejected, or still under consideration. The Change Manager reviews the RFC specifically for the impact to the DCMA infrastructure and makes a recommendation.

c. Assess and Approve RFC. The RFC is presented to the CAB for review and the change is approved or rejected. Approved changes are tentatively scheduled for implementation pending 4ENO CAB approval.

d. Create 4ENO Change Request. The Change Manager creates a change request on the 4ENO portal.

e. Assess and Approve Change Request. The 4ENO CAB assesses, approves, or rejects the DCMA Significant Impact Change Request.

f. Receive 4ENO CAB Approval. The Change Manager assigns the RFC to the Change Implementer.

g. Implement Change. The Change Implementer deploys the change.

h. Validate Change. The Change Requester validates the implementation and submits it for review and closure.

i. Review and Close. The Change Manager closes the RFC after review and verification that activities and tasks have been completed.

SECTION 7: CfM GENERAL PROCEDURES

The CfM team and key stakeholders decide what level of CfM is required to support the services delivered by the organization, how this level will be achieved, and formally document this process in a CfM plan. While this activity is usually performed once (when the process is first being implemented), it is good practice to periodically review the CfM plan to ensure that the process remains relevant to support the needs of the organization.

7.1. CfM PLANNING AND DESIGN. The CfM plan documents the approach to control, identify, record, and report IT components, including versions (where appropriate), constituent components, operational states and most importantly, relationships to other IT components and services. This ensures execution supports all other Service Management processes, such as Release Management, ChM, Incident Management, Problem Management, Capacity Management, and facilitates development and coordination. The "Planning and Design Process Flow" is located on the Resource Page.

a. **CfM Plan.** The DCMA CfM Plan will be unique and based on the level of detail needed to support the services it provides. The CfM plan will be located on the Resource Page.

b. **CMDB Structure.** Defining the DCMA CMDB structure is a key activity that contributes in making the CMDB a powerful decision support tool. The CMDB structure will contain the various CI classes and their relationship to one another in the delivery of a service.

c. **CI Selection Guidelines.** The selection of CIs and level to which they are defined and controlled are very important decisions to be made in the design of the CMDB. CIs will be selected by applying a top-down approach, considering whether it is sensible to break down a CI into component CIs or not. CI information will facilitate the management of change, the control of incidents and problems, and the control of assets that can be independently moved, copied or changed.

d. **Populate CMDB.** This activity involves the creation of CI records in the CMDB for each CI that has previously been identified as part of the initial CMDB build.

(1) Evaluate the request and determine the new CI type to be created based on the CI selection guidelines documented in the CfM plan.

(2) Assign a unique identifier to the new CI type identified.

(3) Identify the necessary attributes for the new CI type.

(4) Specify the appropriate relationships required for the new CI type.

(5) Publish the new CI type in the production CMDB.

e. **Baseline CMDB.** To facilitate tracking of the different changes that will be made in the CMDB, it is recommended that a baseline of the audited CIs be made before moving the initial data into the production instance.

7.2. CONFIGURATION IDENTIFICATION. This activity determines the scope and criteria of CIs to be included in the CMDB. This includes the modeling of the infrastructure to determine what CIs will look like and how they are related to each other. It also includes establishing naming conventions, enterprise taxonomy and CI selection criteria. The "Configuration Identification Process Flow" is located on the Resource Page.

7.3. CONFIGURATION CONTROL. Configuration control is the activity responsible for ensuring that only authorized and identifiable CIs are in the infrastructure and that there is a corresponding accurate and complete CI record representing the CI in the CMDB. Updates to the CMDB are governed by Configuration Control activities. Unauthorized changes are forwarded to ChM for instructions on how to proceed. Discrepancies and errors in the CI configuration are forwarded to the CI Owner for resolution. The "Configuration Control Process Flow" is located on the Resource Page.

a. **Validate Update Request.** The Configuration Process Manager receives a request to enter a new CI record or update an existing CI record. Authorized requests are prioritized and forwarded to a ChM analyst for further processing. Rejected requests are returned to the requester with an explanation of the rejection. In the case of new CIs identified by discovery, verify that an authorized request exists to justify the presence of the discovered CIs.

b. **Validate CI Attributes.** For new CI requests, validate that the proposed CI attributes meet the requirements of configuration management as defined in the configuration management plan.

1. If all the proposed CI attributes meet the criteria, the request is approved to update the CMDB.

2. For CI attributes that fail to meet the configuration management plan criteria, reject the request and inform the CI Owner with proper instructions.

c. **Review Invalid Attributes.** Review the submitted instructions for defining proper CI attributes and submit a new request.

d. **Update CMDB.** Publish the valid and authorized CI data into the CMDB.

7.4. STATUS ACCOUNTING AND REPORTING. This is the production of reports on the current, past and future status of the infrastructure and the CIs under the control of configuration management. The "Status Accounting and Reporting Process Flow" is located on the Resource Page.

a. **Approve Or Reject Report Request.** Review the submitted report request and validate if the request is for an existing report or gauge.

b. **Create Or Update Configuration Management Report.** For valid requests, create new configuration report or gauge as requested.

c. **Publish Configuration Management Report.** Publish the created report or gauge and send the provided link to the requester.

7.5. VERIFICATION AND AUDIT. This activity involves the review and verification of the physical existence of CIs to check that they are correctly recorded in the CMDB. When discrepancies are found, CfM consults ChM for instructions on what corrective action to execute. There are two possible actions, update the CMDB to reflect what is actually in the infrastructure or change the CI to match the CMDB. The "Verification and Audit Process Flow" is located on the Resource Page.

a. **Approve Or Reject Verification Request.** A request for verification and audit is reviewed and approved or rejected by the Configuration Process Manager. Rejected requests are returned to the requester with an explanation.

b. **Execute Audit.** Depending on the scope of the verification or audit request, the Configuration Analyst performs an audit via physical inspection or discovery.

c. **Reconcile With Cmdb.** Review the compiled results from the audit and compare with CI record information found in the production CMDB.

d. **Determine Corrective Action.** If discrepancies exist between the information contained in the CMDB and the actual CIs, there are two possible actions to take:

(1) Update the CMDB to reflect what was verified in the infrastructure.

(2) Change the CI to match the information in the CMDB

(3) The task of correction is passed to the CI Owner.

e. **Initiate Corrective CMDB Action.** Update the CMDB so that the CI record matches the "As Is" CI configuration in the infrastructure.

f. **Execute Corrective Action.** Change the configuration of the actual CI so that it matches the CMDB CI record.

GLOSSARY

G.1. DEFINITIONS.

4ENO. The consolidation and optimization effort for the fourth estate will involve numerous functions**,** including networking, computing, licensing, IT service management and anything else needed to get to a single classified and a single unclassified network,

CfM. The purpose of the CfM process is to control, identify, record, and report IT components, including versions (where appropriate), constituent components, states and most importantly, relationships to other IT components and services.

Change Authority. The Change Authority reviews change requests, rejects requests with insufficient information, leads CAB meetings, identifies relevant CAB members, acts as liaison in order to coordinate changes. For Normal RFCs, the CAB is the Change Authority. For Emergency RFCs the ECAB is the Change Authority. The CAB approves the Change Authority for Standard RFCs.

Change Evaluation. Change Evaluation is a formal evaluation process that is conducted prior to the execution of any significant change. The organization determines the definition (threshold) of significant changes that invoke this process. The goal of Change Evaluation is to provide accurate information to the ChM process as to the impact and effect the change may have on service capability prior to acceptance of the change.

Change Implementer. The owner of the change – if the change requester is someone else. The Change Implementer coordinates with the change requester for business/technical queries and issues. They check and decide an implementation date, ensuring that it doesn't conflict with other activities. They assess and manage the risk involved, test and implement the change, and coordinate and communicate with the other impacted team prior to submitting the change. Once the change is approved, execute the change on the scheduled date and time, document the change procedure, and provide closure status. (GreyCampus 2015)

Change Manager. The Change Manager acts as a facilitator, responsible for the overall change management process. Their primary responsibilities are to authorize and approve minor/low-risk changes, authorize and/or reject changes, and chair CAB meetings to discuss higher risk changes. The Change Manager leads CAB meetings, identifies relevant CAB members, acts as liaison, reviews implemented changes, manages Production Implementation Review, closes RFCs, and delivers management reports. The Change Manager ensures that all the activities designed to implement the change are as per the standards, and prepares the Change Summary Sheet that summarizes all RFCs. This sheet helps the CAB team to understand and evaluate the proposed change. (GreyCampus 2015)

ChM. The purpose of the ChM process is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner. To this end, ChM ensures that any modification to the IT environment, whether it involves an addition, maintenance, or deletion of a service or service component, is in line with the overall mission strategy. This process

provides standardized methods and procedures for efficient and prompt handling of technical changes, to minimize the impact of change-related incidents to service quality, and improves day-to-day operations of the organization.

CMDB. The CMDB is a fundamental component of the Information Technology Infrastructure Library (ITIL) framework's CfM process. CMDBs are used to keep track of the state of assets such as products, systems, software, facilities, people as they exist at specific points in time, and the relationship between all assets. A CMDB helps an organization understand the relationship between the components of a system and to track their configurations. The maintenance of this information allows for certain actions, such as the reconstruction of assets, to occur at any point in time. CMDBs can also be used for things like impact analysis, root cause analysis, or change management.

Configuration Process Manager. Coordinates the allocation of resources and/or responsibilities, while ensuring that all relevant staff have the required technical and business understanding, knowledge and training in the process, and are aware of their role in the process. Provides the description, mission statement, roadmap, strategy, process objectives and metrics to measure success and obtain formal approval for the process and its associated procedures.

GOV. IT GOV is a compilation of all GOV activities, people, GOV bodies, policies, documentation, templates, strategy, charters, and models in a holistic framework that provides visibility and positive command and control of the organization. Many of the components are built during creation of the strategy, operating guide development, and project execution activities.

ITSM. ITSM refers to the entirety of activities – directed by policies, organized and structured in processes and supporting procedures – that are performed by an organization or part of an organization to plan, deliver, operate and control IT services offered to customers.

Major Change. Changes to the operating environment impacting 70 percent or more of the Agency infrastructure

Service Management System. Service management systems are large modular systems which incorporate all or most aspects of a service-oriented organization such as incident, problem, ChM, and CfM.

Significant Change. Changes to the operating environment impacting 50 percent or more of the Agency infrastructure

GLOSSARY

G.2. ACRONYMS.

4ENO	Fourth Estate Network Optimization
CAB	Change Advisory Board
CfM	configuration management
ChM	change management
CI	Configuration Item
CMDB	Configuration Management Database
ECAB	Emergency Change Advisory Board
GOV	governance
IT	Information Technology
IT-SLT	Information Technology-Senior Leadership Team
ITSM	Information Technology Service Management
RFC	Request for Change

REFERENCES

DoD Directive 5105.64, "Defense Contract Management Agency (DCMA)," January 10, 2013
DoD Directive 8440.01, "DoD Information Technology Service Management," December 24, 2015
GreyCampus. 2015. *ITIL Change Management Roles and Responsibilities.* March 20. Accessed August 15, 2018. https://www.greycampus.com/blog/it-service-management/itil-change-management-roles-and-responsibilities.