Common User Baseline for the Intelligence Community (CUBIC) Configuration Management Plan Version 2.0

Air Force Research Laboratory
IFEB
32 Brooks Road
Rome, New York 13441-4114

5 November 1999

SIGNATURE PAGE

Steve Aytes, Col, USAF
Director, Intelligence Systems

John Vona
Chief, Information Handling Branch

TABLE OF CONTENTS

SECTION ONE: SCOPE OF CONFIGURATION MANAGEMENT 1

1.1 Purpose 1

1.2 Objective 1

1.3 Reference Documents 1

1.4 Definitions 2

1.5 Configuration Control Management Structure 5
1.5.1 Program Management Office 5
1.5.2 Program Configuration Control Board (CCB) 5
1.5.2.1 Program CCB Responsibilities 5
1.5.2.2 Program CCB Attendees 6
1.5.2.3 Program CCB Agenda 6
1.5.2.4 Program CCB Minutes 6

1.6 CUBIC Configuration Control Board 6
1.6.1 CCCB Responsibilities 6
1.6.2 CCCB Attendees 7
1.6.3 CCCB Agenda 7
1.6.4 CCCB Minutes 7

1.7 Changes to the CM Process 7

1.8 Information Flow for CUBIC 7

SECTION TWO: CONFIGURATION MANAGEMENT ACTIVITIES 9

2.1 Product Baseline Version Identification 9

2.2 Document/Media Identification 10

2.3 Configuration Control 10
2.3.1 Flow of Configuration Control 10
2.3.2 Configuration Control Documentation 10
2.3.3 Documentation Storage and Control 12
2.3.4 Document Reproduction or Requests 12
2.3.5 Software Storage and Control 12
2.3.6 Software Reproduction or Requests 12

2.4 Configuration Status Accounting 12
2.4.1 CMDB 13
2.4.2 CMDB Access 13

2.5 Configuration Installation and Testing 14

2.6 Metrics 14

2.7 Quality Assurance **14**

SECTION THREE: TEST FINDING (TF) PROCESS **17**

3.1 TF Overview **17**

3.2 TF Process **17**

3.3 Impact Code Descriptions **17**
3.3.1 JITF 17
3.3.2 Security 19

SECTION FOUR: PROBLEM REPORT/CHANGE REQUEST/MULTIPLE APPLICATION PROBLEM/REQUIREMENT (PCMR) PROCESS **21**

4.1 PCMR Overview **21**

4.2 CM Responsibilities **21**

4.3 PCMR Process **22**
4.3.1 Impact Code Descriptions 25
4.3.2 Classification Issues 26
4.3.3 Submission of an Impact Code 1 PR 26

4.4 Summary **27**

SECTION FIVE: DOCUMENT MANAGEMENT PROCESS **32**

5.1 DRR Overview **32**

5.2 DRR Process **32**

5.3 CDRL Tracking Procedures **33**

SECTION SIX: ACTION ITEM PROCESS **36**

6.1 AI Overview **36**

6.2 AI Process **36**

SECTION SEVEN: SOFTWARE RELEASES **38**

7.1 Software Releases **38**
7.1.1 PMO Responsibilities 38
7.1.2 Site Responsibilities 38
7.1.3 CM Responsibilities 39
7.1.4 Development Contractor Responsibilities 39

7.2 Emergency Releases **39**

APPENDIX A 40

LIST OF EXHIBITS

EXHIBIT 1-1. CONFIGURATION CONTROL MANAGEMENT STRUCTURE 8
EXHIBIT 2-1. CMDB ARCHITECTURE 13
EXHIBIT 2-2. IMA CERTIFICATION PROCESS 16
EXHIBIT 3-1. TEST FINDING PROCESS 18
EXHIBIT 4-1. PCMR PROCESS 24
EXHIBIT 4-2. IMPACT CODE 1 PROCESS 27
EXHIBIT 4-3. SAMPLE NOTIFICATION LETTER 28
EXHIBIT 4-4. SAMPLE TASKING LETTER 30
EXHIBIT 5-1. DOCUMENT REVIEW REPORT PROCESS 34
EXHIBIT 5-2. SAMPLE DRR TRANSMITTAL LETTER 35
EXHIBIT 6-1. ACTION ITEM PROCESS 37

PREFACE

This document provides configuration management (CM) direction and applies CM discipline to the development, installation, maintenance, modification, enhancement, and traceability of application software and documentation. The objective of this CM Plan is to describe a process for more effectively developing and maintaining software by improving accountability, reproducibility, traceability, and coordination. The services described in this document can be tailored to meet the needs of an individual program. In addition, Program Management Offices (PMOs) can "pick and choose" which CM services to receive and have maintained. All information contained in this document is superseded by information contained in the program contract regarding the same subject areas. Program managers are encouraged to incorporate the concepts promoted in this document into their software development contracts. The contents of this document are organized as follows:

Section One: Scope of Configuration Management gives the reader an overview of what CM is, what purpose it serves, related terms, and a look at the structure of CM.

Section Two: Configuration Management Activities describes the support function of CM activities and the tool used in tracking necessary life cycle information for a program. The CM activities are key to the organization and effective implementation of CM in the software development process.

Section Three: Test Finding Process describes the process in which findings that are generated during formal integration, interoperability, and security testing are identified, tracked and forwarded to the Intelligence Mission Application (IMA) PMOs.

Section Four: Problem Report/Change Request/Multiple Application Problem/ Requirement Process describes the process in which problem reports (PRs), change requests (CRs), multiple application problems (MAPs), and requirements are generated and tracked. This is a planned and systematic set of techniques, documentation, and actions necessary to control change to individual and related applications.

Section Five: Document Management Process describes how Document Review Reports (DRRs) are a tool used within a program to evaluate, verify, and check the accuracy and adherence to standards for documentation releases. Contract Data Requirements List (CDRL) tracking procedures, which help monitor development of the software and its associated documentation, are also described.

Section Six: Action Item Process describes how action items (AIs) are a management tool used to identify and track issues for supported programs.

Section Seven: Software Releases describes the software release process.

PROGRAM OVERVIEW

The Air Force Research Laboratory (AFRL), Rome Research Site, is home to a number of Department of Defense (DOD) Intelligence Information System (DODIIS) legacy and IMA PMOs and the Joint Integration Test Facility (JITF). AFRL's Information Handling Branch (IFEB), working with the 497IG/IND, provides a unique collection of CM services supporting the Common User Baseline for the Intelligence Community (CUBIC) organization made up of selected software applications.

CUBIC has a strong legacy of supporting the intelligence community through defined processes for problem identification, change control, and quality software distribution. The success of CUBIC is predicated upon extensive user participation throughout the software development cycle. These concepts have evolved since their initial inception to a streamlined, focused, cost effective methodology that assists the PMO in controlling changes to software baselines and provides critical information to multiple users. The foundation of CUBIC is the successful partnership between 497IG/IND and AFRL. The 497IG/IND functions as CM's executive manager and ensures representation of user requirements at upper levels of DOD management. AFRL/IFEB provides CM services to PMOs and their users and supports the 497IG/IND. This process supports PMOs at AFRL, the Electronic Systems Center (ESC) at Hanscom Air Force Base, and CUBIC users. Roles and responsibilities for each of these organizations and CM participants are outlined in this document. The services provided include:

- Using and expanding automated and networked management aids to streamline CUBIC processes and interactions with worldwide users/developers.
- Receiving, processing, and accounting for the status of PRs/CRs, MAPs, Requirements, DRRs, Test Findings (TFs), and AIs.
- Identifying, controlling, and accounting for the status of software configurations.
- Maintaining software and documentation libraries for supported programs.
- Supporting programs with software release and documentation distribution.
- Maintaining application baselines.
- Streamlining and standardizing PMO/user communications by implementing uniform reporting and tracking procedures and practices, including on-line global network data files and interfaces.
- Maintaining and enhancing interoperability between software applications through management oversight at the community level.

The CUBIC process acknowledged almost a decade ago that "stovepipe" development was counter-productive to the success of intelligence community goals. For this select subset of intelligence applications there is guidance for the implementation of major DOD initiatives and downward directed requirements through formal change control procedures. There is also a primary focus on upward directed requirements identified by operational users. The CM process begins and ends with the user and is based upon extensive user involvement. CUBIC provides its users with the mechanisms and support to enhance the performance of the software applications required by the intelligence mission.

SECTION ONE
SCOPE OF CONFIGURATION MANAGEMENT

1.1 PURPOSE

This plan establishes CM policies, methods, and procedures to be implemented and followed to control the configuration of software programs managed by AFRL and ESC. This document supersedes the CUBIC Configuration Management Plan, Version 1.0, dated 25 July 1997.

If you would like additional information on the items discussed in this document, contact CM at the following address and phone number:

Configuration Management
Air Force Research Laboratory/IFEB
32 Brooks Road
Rome NY 13441-4114

DSN 587-2723/4209
COMM 315-330-2723/4209
FAX 315-330-1637

UNCLASS E-MAIL cubic_cm@rl.af.mil
CLASS E-MAIL cubic_cm@romans.rome.ic.gov

INTERNET www.if.afrl.af.mil/programs/cm/
INTELINK web1.rome.ic.gov/cm/

1.2 OBJECTIVE

This CM Plan establishes the guidelines and applies CM discipline to the development, installation, maintenance, modification, enhancement, and traceability of application software and documentation.

1.3 REFERENCE DOCUMENTS

The following documents are referenced in this CM Plan:

- CJCSI 6212.01A, Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems, 30 June 1995.
- Defense Intelligence Agency Regulation No. 65-13, Automated Information System Life Cycle Management.
- DOD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, 15 March 1996.
- DOD Directive 5000.1, Defense Acquisition, 15 March 1996.
- DODIIS Community Transition to Migration Systems, September 1995.
- DODIIS Instructions, April 1999.

- DODIIS Migration Systems Program Management Plan (PMP), September 1994.
- IEEE/EIA 12207.0-1996, Industry Implementation of International Standard ISO/IEC 12207: 1995, March 1998.
- IEEE/EIA 12207.1-1997, Industry Implementation of International Standard ISO/IEC 12207: 1995, April 1998.
- IEEE/EIA 12207.2-1997, Industry Implementation of International Standard ISO/IEC 12207: 1995, April 1998.
- Joint DODIIS/Cryptologic SCI Information Systems Security Standards, 28 March 1997.
- Test and Evaluation Policy for DODIIS Intelligence Mission Applications (IMAs), April 1999.
- User's Manual for the Configuration Management Database (CMDB) Version 1.0, 01 March 1999.

1.4 DEFINITIONS

The following is a list of definitions for terms used in this document.

ACTION ITEM (AI)

A management tool used to identify and track program issues.

ADDRESS INDICATOR GROUP (AIG)

A collection of Automatic Digital Network (AUTODIN) message Plain Language Addresses (PLAs) for a related group of users. The relationship can be a common software application, mission, or organizational alignment (such as all DODIIS users). An AIG facilitates a quick and efficient means of communication between the PMO and users, keeping everyone cognizant of issues that concern a program.

AUTODIN is being replaced by the Defense Messaging System (DMS) at the end of 1999.

CHANGE REQUEST (CR)

A new requirement or enhancement that is not part of the baselined software requirements.

COMPATIBILITY

The capability of two or more items or components of equipment or material to exist or function in the same system or environment without mutual interference.

CONFIGURATION MANAGEMENT DATABASE (CMDB)

An automated status accounting tool used to record and report information related to supported programs by CM.

DEVELOPMENT CONTRACTOR

The organization or company that does the actual development of the software.

DOCUMENT REVIEW REPORT (DRR)

A tool used within a program to evaluate, verify, and approve or disapprove the accurate adherence to standards within program documentation.

DODIIS EXECUTIVE AGENTS (DEXAS)

Office [Service, Agency, or Unified & Specified (U&S) Command] responsible for management and requirements oversight of one or more IMAs.

EXECUTIVE MANAGER

Office responsible for requirements oversight of one or more programs. If there is a DEXA for the program, they are the executive manager. Program requirements are verified and validated by the executive manager.

INTEGRATION

The arrangement of systems in an architecture so that they function together in an efficient and logical way.

INTELLIGENCE MISSION APPLICATION (IMA)

An automated information system within a corporate information management functional area that has been selected or designated as the standard application to support standard processes for a functional activity or sub-activity, formerly known as migration systems.

INTERFACE

The functional and physical characteristics required at a common boundary between two or more hardware/software products.

INTEROPERABILITY

The ability of the systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together. The conditions achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.

LEGACY SYSTEM

An application whose critical functionality will be subsumed by an IMA or an application that duplicates the functions of an IMA and is scheduled to be terminated, e.g., DAWS and MAXI.

LIBRARY

A centralized collection of all supported program documentation and software as part of CM services. Documents are available hardcopy, softcopy, or on-line. The library maintains the current and two previous versions of software release documentation.

MULTIPLE APPLICATION PROBLEM (MAP)

The mechanism used to coordinate interface changes between applications when a PR or CR affects multiple applications, formerly known as a Request for Change (RFC).

NOTIFICATION LETTER

A formal request from the PMO to the contracted developer requesting a written plan on the level of effort to implement a change to the software.

PLAIN LANGUAGE ADDRESS (PLA)

An address consisting of the site name, its location, and any appropriate office symbols, e.g., AFRL ROME NY//IFEB//. Each office symbol listed on an AUTODIN message PLA will receive a copy of all messages addressed to the AIG.

POINT OF CONTACT (POC)

The focal point for an application.

PROBLEM REPORT (PR)

A report describing a software deficiency whereby the software does not function as documented by the program requirements.

PROFILE

A profile is a collection of information maintained by CM to define a user, site,

organization, PMO, or developer. The profile contains information on POCs, street and electronic mailing addresses, phone numbers, AUTODIN message PLAs, facsimile numbers, and programs of interest.

PROGRAM

All the activities and processes involved in creating an application, formerly known as a subsystem or segment.

PROGRAM MANAGEMENT OFFICE (PMO)

The PMO is responsible for developing an acquisition strategy, planning the program by developing a management approach, budgetary estimates and alternatives, program schedules, contract strategies and structures, and conducting the day-to-day management of the program's development, enhancement, or maintenance. The PMO is also responsible for directing the development contractor and ensuring adequate testing of the application to minimize the number of errors experienced by users.

PROGRAM USER GROUP

A group to provide a forum for information exchange between the users and program management. The users can make recommendations to the PMO as appropriate. During user group meetings, representatives from program management, users, and contractor(s) meet to discuss program specific issues. These issues may include, but are not limited to; program status, proposed enhancements, problems and concerns, CM, user issues, and demonstrations. Program user group meetings are normally held semi-annually and can be hosted by the PMO or at a designated location.

REQUIREMENT

Information maintained by CM to track program level requirements for future versions. These requirements translate to program specifications.

SITE

The physical location where software applications are installed and operated by users.

SOFTWARE PROBLEM REPORT (SPR)

A report describing a software deficiency whereby the software does not function as documented by program requirements during design reviews and development contractor-run testing.

SOFTWARE RELEASE

A software release is made up of the software application media and associated documentation. CM tracks and stores detailed information regarding software releases and supports reproduction and distribution of releases for programs.

SOFTWARE VERSION DESCRIPTION (SVD)

The document that identifies the exact version and contents of the software release packages and contains the following information: document identification, inventory and description of release package contents, PR/CR change summary, and interface compatibility.

TASKING LETTER

Formal tasking from the PMO to the development contractor to implement a software change into a specified version of software.

TEST FINDING (TF)

A software or document deficiency identified during formal testing, i.e., JITF, Joint Interoperability Test Command (JITC), or Security, of IMAs.

USER

Any organization or individual that operates or is affected by software applications supported by CM.

VENDOR

An organization or company that supplies Commercial-Off-The-Shelf (COTS) and/or Government-Off-The-Shelf (GOTS) software to the government.

WORKPLAN

A document that identifies the estimated level of effort required to implement a software change and is the formal response to a Notification Letter.

1.5 CONFIGURATION CONTROL MANAGEMENT STRUCTURE

1.5.1 PROGRAM MANAGEMENT OFFICE

The PMO identifies and evaluates advanced concepts and initiatives for the software and provides research, development, and enhancement engineering for Preplanned Product Improvement (P^3I) for software in accordance with published standards.

In addition to providing research and development for the software, the PMO is also responsible for all aspects of CM for the program. All PRs/CRs/Requirements, DRRs, program documentation, AIs, user profiles, and software release information are logged and monitored using the CMDB, which provides automated tracking. The PMO also provides quality assurance (QA), ensuring that the software and documentation conform to established technical and functional requirements, including all aspects of testing, development and operational software.

1.5.2 PROGRAM CONFIGURATION CONTROL BOARD (CCB)

The purpose of a program CCB, with an executive manager as chairperson, is to provide a focus for change control. Meetings are called as required. Exhibit 1-1 illustrates the relationship between the PMO, CCB, developer, users, and executive managers.

1.5.2.1 Program CCB Responsibilities

The Program CCB is usually responsible for the following activities:

- Enforces policy for life cycle management of the program.
- Determines the program's response to MAPs submitted by other CUBIC programs.
- Approves/disapproves and prioritizes all PRs/CRs by user survey with the final decision made by the CCB Chairperson. PRs are voted on at the discretion of the individual programs.
- Evaluates if approved CRs will initiate a MAP due to impact on interfaces or infrastructure.
- Approves/disapproves completed program MAP packages. Program approved MAP packages that have cost and schedule impact to the intelligence community are forwarded to the CUBIC CCB (CCCB) for approval/disapproval. Approved MAPs with no cost and schedule impact are implemented at the

program manager's discretion, in coordination with the executive manager.

1.5.2.2 Program CCB Attendees

- ❑ Program executive manager
- ❑ Program manager (PM) or PMO representative
- ❑ AFRL or ESC Division Chief
- ❑ Site representatives
- ❑ Developer(s)
- ❑ Program support contractors, i.e., System Engineering and Technical Assistance (SETA), Independent Verification and Validation (IV&V), Technical and Engineering Management Support (TEMS)
- ❑ CM representative (AFRL)
- ❑ CUBIC executive manager (497th IG)

1.5.2.3 Program CCB Agenda

CCB agendas are mandatory. The following is a suggested format:

- ❑ Old action item status review.
- ❑ Review of program interface matrices.
- ❑ Present and discuss new issues including status reviews of MAPs and CRs.
- ❑ Present and discuss recommendations.
- ❑ Evaluate and determine responses to MAPs submitted by other programs.
- ❑ Approval/disapproval of changes to baseline, e.g., CRs and program initiated MAPs.
- ❑ Review of decisions and action items.

1.5.2.4 Program CCB Minutes

Minutes of the proceedings, including a list of action items, will be taken by a representative of the program and submitted to the chairperson for approval within 10 working days after the meeting. Distribution to all attendees will occur within five (5) working days of the chairperson's approval. Program Manager's and Chairperson's signatures are required on minutes.

1.6 CUBIC CONFIGURATION CONTROL BOARD

The purpose of the CCCB, with the 497IG/IND as chairperson, is to address problems outside the purview of the Program CCBs, problems unsolvable by the individual Program CCBs, and those problems and changes which affect multiple applications. A charter will be developed for the CCCB. The CCCB provides oversight for programs supported by CM and ensures that common problems are solved by common solutions in keeping with open systems philosophy. This is the highest level of oversight in the CM process.

1.6.1 CCCB RESPONSIBILITIES

- ❑ Makes decisions on issues beyond the scope of Program CCBs, yet within the scope of the overall CUBIC program.
- ❑ Approves or disapproves all interfaces, and related issues, to or between supported programs, except

those interfaces determined by the CCCB to be command specific.

- ❑ Approves or disapproves MAPs beyond the scope of the affected supported program CCBs.
- ❑ Forwards MAPs beyond the scope of the CCCB to the appropriate organizations.
- ❑ Reviews all program CCB minutes and reports.

1.6.2 CCCB ATTENDEES

- ❑ Air Force Research Laboratory Information Handling Branch Chief
- ❑ CM representative (Air Force Research Laboratory)
- ❑ CUBIC executive manager (497th IG)
- ❑ Program managers or PMO representative
- ❑ Program executive manager
- ❑ Security representative(s)
- ❑ Training representative(s)

1.6.3 CCCB AGENDA

CCCB agendas are mandatory. The following is a suggested format:

- ❑ Old action item status review.
- ❑ Present and discuss new issues including status reviews of MAPs.
- ❑ Present and discuss recommendations.
- ❑ Approval/disapproval of MAPs.
- ❑ Review of decisions and action items.

1.6.4 CCCB MINUTES

Minutes of the proceedings, including a list of action items, will be taken by a representative of the CUBIC executive manager, such as a support contractor, and submitted to the chairperson for approval within 10 working days after the meeting. Distribution to all attendees will occur within five (5) working days of the chairperson's approval. The Chairperson’s and Information Handling Branch Chief's signatures are required on the minutes.

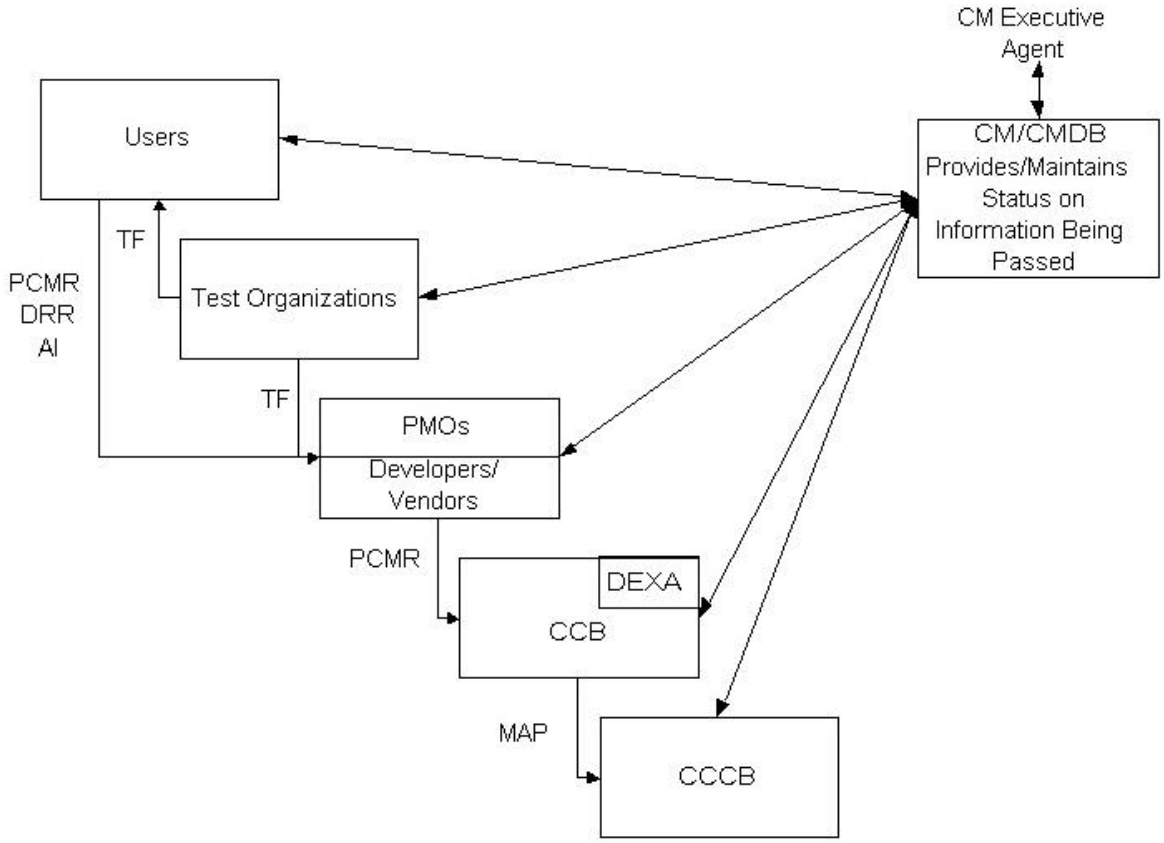
1.7 CHANGES TO THE CM PROCESS

This CM Plan is a living document in that the processes described are continuously evaluated to determine if enhancements are possible. Changes to the policies described in this document are implemented after coordination with the CM program manager, CM executive manager, and the Chief of the Information Handling Branch. The Branch Chief oversees virtually all of the programs currently supported by CM, and is, therefore, a part of the process. PMOs and sites are encouraged to submit their suggestions for enhancements, new services, or other changes to the CM office for consideration using the DRR process, described in Section 5.

1.8 INFORMATION FLOW FOR CUBIC

As described in the previous paragraphs, the CM process ensures that issues are resolved at the lowest effective level. Exhibit 1-1 provides a visual depiction of the types of information managed by CM, information sources, and resolution paths.

Exhibit 1-1. Configuration Control Management Structure



SECTION TWO
CONFIGURATION MANAGEMENT ACTIVITIES

This section describes CM activities and its function of tracking necessary life cycle information for a program. These activities are the key to the organized effective implementation of CM in the software development process:

- Product Baseline Version Identification
- Document/Media Identification
- Configuration Control
- Configuration Status Accounting
- Configuration Installation & Testing
- Metrics
- Quality Assurance

2.1 PRODUCT BASELINE VERSION IDENTIFICATION

Software baselines and releases will be identified with a designator comprised of an integer to provide sequential numbering and decimal numbers indicating revision or version level. The first operational baseline version of the software will be identified with the designator 1.0.

A major release, e.g., 1.0 to 2.0, indicates a significant change in the architecture or operation of the application. A "rough rule of thumb" for PMOs to use for a significant change is 30 percent of the baseline changes. A minor release of a software version is indicated by a change in the decimal number, e.g., 1.0 to 1.1. A minor release includes new features but the fundamental architecture remains unchanged. A maintenance release, e.g., 1.1.1, indicates new features may have been added, but the emphasis is on optimization, feature enhancements, or modifications to improve stability and usability. All release numbers are determined by the PMO.

The Software Version Description (SVD) will identify the exact version and contents of the software release package. As a minimum, the SVD will contain the following information:

- Release document identification
- Inventory and description of release package contents
- PR/CR change summary and notes

- Interface compatibility

2.2 DOCUMENT/MEDIA IDENTIFICATION

All documents and media stored in the CM library will be assigned a unique one-up control number.

The PMO will apply appropriate Government or standard commercial labels on all magnetic media. These labels should show the application name, media title, date of media, classification, contractor name (if appropriate), and contractor media tracking number (if appropriate).

2.3 CONFIGURATION CONTROL

Configuration control encompasses the process of authenticating configuration identification documents and the processes by which changes are systematically requested, evaluated, classified, approved/disapproved, and subsequently implemented. Once the application components have been identified, configuration control measures assist in ensuring the established identification and allocation are preserved and no unauthorized changes are made to the application. Configuration control requires that changes to controlled configuration items (CIs) be submitted, evaluated, approved or disapproved, implemented, verified, and released according to established CM procedures. This aids in keeping configuration identification current and provides a reliable reference point for subsequent changes and development efforts. Once a baseline is established, the CIs constituting that baseline are subject to change control by the PMO.

2.3.1 FLOW OF CONFIGURATION CONTROL

Configuration control calls for the documentation of all proposed changes; evaluation of these changes for cost, schedule, document and design impact, and orderly implementation of changes. The configuration control process consists of three (3) basic steps:

- *Step One - Initiation of the Change.* Proposed changes to the baseline are recorded as PRs/CRs/DRRs and assigned a unique identifier.

- *Step Two - Investigation and Review of Proposed Change.* The PMO validates every PR/CR/DRR. If the proposed PR/CR/DRR affects interfaces to other programs or external systems, the PMO will initiate a MAP to determine the impact to other PMOs and coordinate the proposed change. (PR/CR/MAP verification is discussed in Section 4 and DRRs in Section 5.)

- *Step Three - Implementation of Approved Changes.* Approved changes are scheduled for incorporation and implemented based upon priorities established by the executive manager and any other outside influences based upon an interface issue.

2.3.2 CONFIGURATION CONTROL DOCUMENTATION

All proposed changes to the software and documentation will be submitted for consideration using the approved change control reporting formats. The following forms will be used to record and track changes:

Deviation: A configuration deviation is a specific written authorization granted prior to the manufacture of a computer program to depart from a particular performance or design requirement of a specification, drawing, or other document for a specific number of units or period of time. A deviation does not require revision of the applicable specification or drawing. A deviation may be converted to an Engineering Change Proposal (ECP) if it is determined that the change should be permanent. Deviations should not be submitted or authorized that affect service operation, logistics, interoperability, or maintenance. PMOs, in coordination with their program executive manager, approve or disapprove deviations. If the nature of these changes affect other programs or interfaces, the PMO should determine if a MAP is required.

DRR: A DRR is used during document reviews, design reviews, and testing to record problems found in any program documentation. DRRs may be initiated by any participant in the review of the documentation. They are tracked by the PMO via CM to ensure required changes are incorporated into the documentation. DRRs are discussed fully in Section 5.

ECP: A contract ECP can be used, depending upon the contract, to request an alteration in the configuration of an item that is delivered, to be delivered, or under development, after formal establishment of its configuration identification. An ECP shall be submitted to the Government by the developer on DD Form 1692, Engineering Change Proposal. It may be supported by annotated copies of technical documentation and other information as required to justify and describe the change. ECPs are approved or disapproved by the PMO, in coordination with the executive manager, based upon the severity of the change. If the nature of these changes affect other programs or interfaces, the PMO should determine if a MAP is required.

MAP: A MAP coordinates changes that affect multiple applications. MAPs are logical extensions to the change control process and acknowledge that applications are no longer built as “stovepipes” and that all problems and changes cannot be resolved within a single PMO. The MAP process coordinates changes between CM supported programs and other DODIIS applications, non-DODIIS, and COTS products. MAPs are discussed fully in Section 4.

PR/CR: A PR/CR is the means by which users report problems encountered with the baselined versions of the software, make suggestions as to how the software can be made more efficient, or to request changes for enhancements. Section 4 contains detailed information on the processing of PRs/CRs.

SPR: A SPR will be used during design reviews and development contractor-run testing to record software errors. SPRs may be initiated by any program participant. SPRs generated during formal government acceptance testing, e.g., inplant, are monitored by the PMO to ensure necessary corrective action is accomplished and that changes are properly incorporated into the software. SPRs not resolved prior to acceptance of software will be converted into PRs/CRs for tracking.

TF: A TF is a means by which testers report a software or document deficiency identified during formal testing, i.e., JITF, JITC, or Security, of IMAs. Test Findings are discussed in Section 3.

Waiver: A configuration waiver authorizes the acceptance of an item that varies from the baseline standards after final testing or at

the start of production. PMOs, in coordination with their executive manager, approve or disapprove waivers. If the nature of these changes affect other programs or interfaces, the PMO should determine if a MAP is required.

2.3.3 DOCUMENTATION STORAGE AND CONTROL

A hardcopy and softcopy of program documentation should be forwarded by the PMO for inclusion into the CM library. Upon receipt, documents are logged into the CMDB. The current and two previous versions is retained. This will be done for change pages as well. Classified documentation will be controlled by AF Form 310, Document Receipt and Destruction Certificate. The receipt, storage, reproduction, and destruction of classified documents will be in accordance with established government security procedures.

All documentation (new or revised) will be reviewed by the PMO in accordance with the documentation review procedures outlined in Section 5. Disapproved documentation will be returned to the development contractor, along with DRRs, for incorporation into the next revision.

2.3.4 DOCUMENT REPRODUCTION OR REQUESTS

Requests for copies of library documentation will be based upon need-to-know as determined by the PMO in coordination with their executive manager. Borrowing hardcopy documents is preferred, but reproduction by CM is available on an as-needed basis. If the documentation is available in softcopy, it can be electronically mailed as long as the file size is less than 5 MB. An approved documentation set will be sent to users with the release of a new baseline.

2.3.5 SOFTWARE STORAGE AND CONTROL

The development contractor stores all software under development for a given program, as part of the development configuration. CM will store PMO accepted software as the product baseline. As a minimum, a master copy of all baselines currently in operational use should be stored at all times in CM.

2.3.6 SOFTWARE REPRODUCTION OR REQUESTS

Requests for copies of library software will be based upon need-to-know as determined by the PMO in coordination with their executive manager. CM has the ability to duplicate CDs, 4mm and 8mm tapes, and diskettes. If program related items need to be duplicated, CM will duplicate and distribute. If a copy of a COTS product is required, proof of license needs to be provided with the request. If an immediate backup of a program related software item is required, this can also be accomplished.

2.4 CONFIGURATION STATUS ACCOUNTING

Status accounting oversees all aspects of CM processing and requires all participants to follow a pre-established workflow. Adherence to this workflow will ensure that status accounting products (PR/CR/Requirement/DRR/AI/Library database, acknowledgment messages, and status reporting) will be accurate and timely. All information regarding the life cycle of the configurable items are logged and tracked using the CMDB for each program, including action dates for notification letters, workplan receipt dates, and tasking letters.

Concurrence information and cross references to related items are also logged.

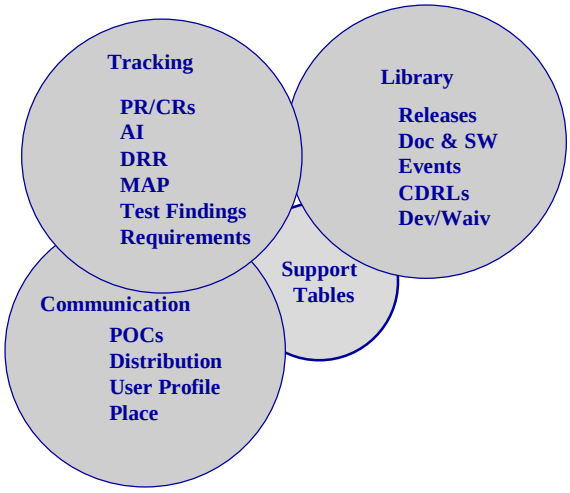
2.4.1 CMDB

The CMDB is the automated status accounting tool used to record and report information. The CMDB is a relational database with a web browser front-end. There are two servers; one on the Internet and the other on Intelink. Access is controlled by user accounts and passwords. Users can view and submit information directly from/to the database. A hardcopy report can be provided to sites upon request who do not have Internet/Intelink access.

Automated requirement tracking tools, like the CMDB, provide current real-time information to the PMO regarding the status of the program. The CMDB also provides insight into the application in order to control change and assist in the production of the highest quality software products possible.

The CMDB component architecture is illustrated in Exhibit 2-1. For additional information on these components, refer to Sections 3, 4, 5, 6 and 7. Additional information on the CMDB can be obtained in the CMDB Users' Manual available upon request from the CM library.

Exhibit 2-1. CMDB Architecture



2.4.2 CMDB ACCESS

New users are required to complete a profile detailing their address, phone, facsimile, unclassified E-mail, POC and AIG status, and what program information they want to access. Notification of new profiles will be sent to each application's PMO that the user has subscribed to for approval and to CM for account creation. Once approval has been granted and CM has created an account, each user will then be assigned a login id and password. The user will be e-mailed or mailed their account Login IDs and assigned an authorization number that CM will track. The user should then call CM with this authorization number for verification and then the user will be given their password.

Profile information is an essential part of the CMDB. Accounts are created according to roles and permissions. A user's login and personal information will be maintained through his/her individual Profile.

Each profiled user of the CMDB will be assigned a specific role for each application the individual has subscribed to within their profile. Specialized access (Read, Add, Modify, or Delete) to the database will be determined by the permissions assigned to that specific role. Only the PMO can assign

these roles based on what the user has a need to know.

POCs provide information used to identify focal points for applications that are responsible for an application at a given location. The information in the POCs is used for preparing software release distribution packages, distributing PR/CR reports and updates, and assisting in the evaluation of program PRs/CRs. Up to date POC information is critical in ensuring the timely distribution and receipt of new software and program information.

2.5 CONFIGURATION INSTALLATION AND TESTING

All current programs supported by CM follow the procedures in the IMA Certification Process, shown in Exhibit 2-2. This process is based on DOD 5000.2-R Lifecycle Management. These programs use SPRs, TFs, PRs/CRs, DRRs, and AIs to track problems with software and documentation identified in the course of testing. This process provides assurance that intelligence applications work as planned when they are delivered to sites. Additional details on the IMA Certification Process can be found in the DODIIS Instructions and the Test and Evaluation Policy Guidance documentation (See paragraph 1.3).

CM or the contractor, per contract requirements, will deliver approved release packages to the sites. The sites will install and test the release packages to validate successful installation and correction of the applicable PRs/CRs. The site is responsible for testing and validating the incorporation of PRs/CRs listed in the SVD. Refer to Section 7 for more information on software releases.

2.6 METRICS

CM will use information stored in the CMDB to generate metrics to provide insight into CM processes, assess variation between releases, and generate information on the software development process. Examples of these metrics include, but are not limited to:

- Length of time a PR/CR remains open in the system.
- Length of time from workplan approval to closure for PRs/CRs.
- Installation rate of new releases.

This information will be provided, upon request, to the PMO, executive manager, CCCB Chair, etc.

2.7 QUALITY ASSURANCE

Many times software development problems can be attributed to the lack of software QA controls. QA, as applied to software, is the systematic evaluation of software and related documentation by an independent person within the program's software development team. The implementation of a tailored QA effort to support software development and maintenance should result in a more orderly process, and permit errors to be found early in the development cycle.

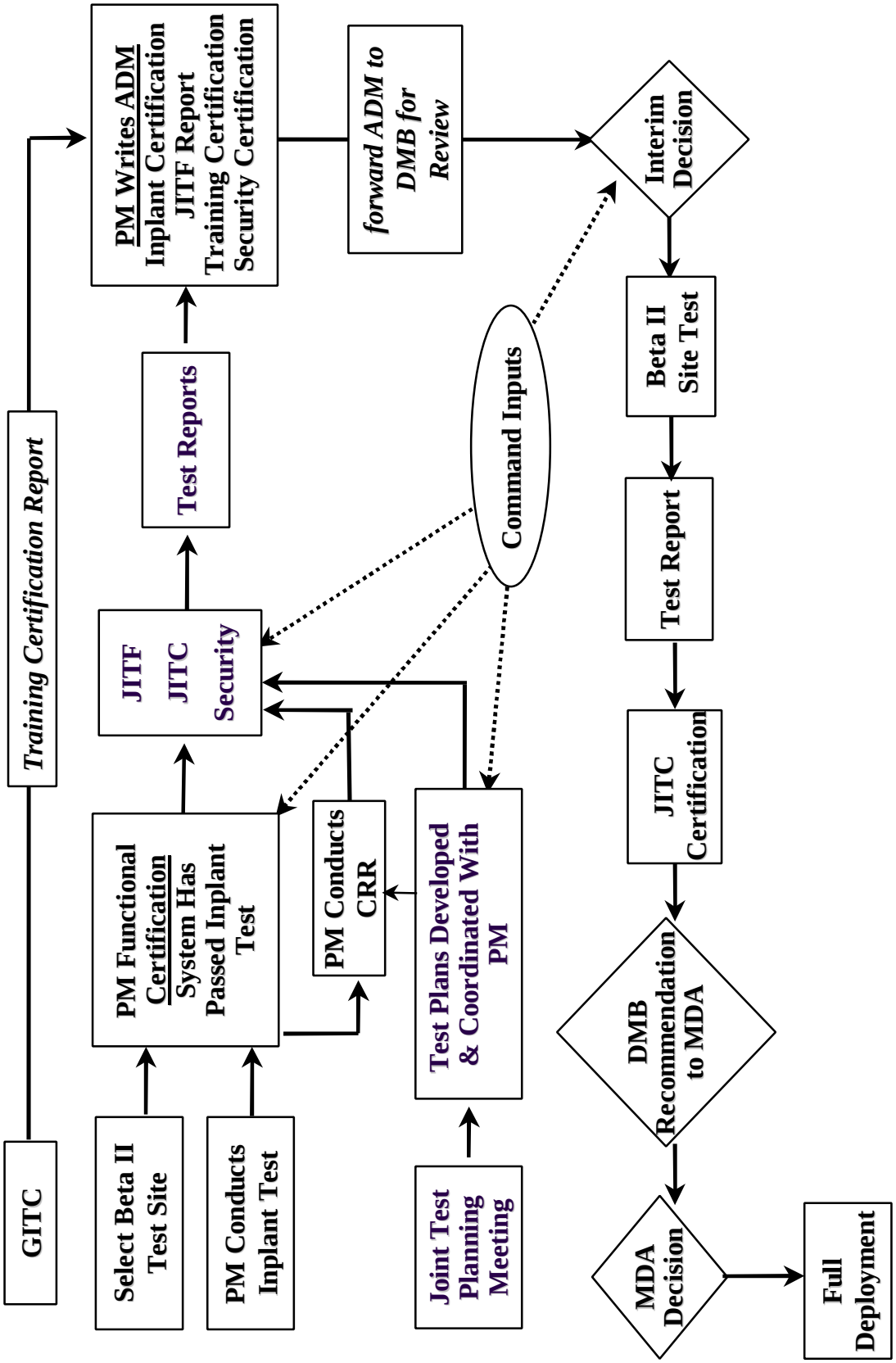
Software development that does not demonstrate the required maturity or completeness as judged by QA controls will be stopped until the documented discrepancies (PRs/CRs, SPRs, TFs, and DRRs) are corrected and incorporated into the development. SPR, TF, and PR/CR QA is a planned set of maintenance procedures, documentation, and actions necessary to provide adequate confidence that the software will perform satisfactorily in actual operations. For example, a software release

with at least one Impact Code 1 PR or SPR discovered during in-plant testing will not proceed to the next phase, e.g., JITF, JITC, or security accreditation. Proceeding would waste time and money since it is already known that the application cannot be used operationally. A major design flaw discovered during review means that the system should not enter the coding phase.

There is no software development strategy that suggests that QA must be performed only on programs during their original development phase. All programs generate SPRs, TFs, and PRs/CRs in which coding errors are discovered during development and operation, regardless of the age or complexity of the software version.

Implementing QA can result in a higher quality product, with greater visibility into the development process and a better understanding of user/customer needs. Although QA has been described as a formal process, it can be done informally by anyone with an objective, independent look at the software development for the program.

Exhibit 2-2. IMA Certification Process



SECTION THREE
TEST FINDING (TF) PROCESS

3.1 TF OVERVIEW

The objective of this process is to ensure that all findings discovered during formal testing, i.e., JITF, JITC, or Security, are tracked and made available to the PMO, decision makers and application users.

3.2 TF PROCESS

The TF process, as illustrated in Exhibit 3-1, provides coordination between all pertinent parties, ensuring that findings from formal testing are properly tracked and implemented. The following is the process in which TFs are identified, tracked, and disseminated.

- ❑ *Step 1* - A finding is identified during testing and submitted by the tester using the inputs forms in the CMDB. If the TF is classified, the tester must submit it by using the input forms on Intelink.

- ❑ *Step 2* – Once testing is complete, the Test Director and CM review the TFs for accuracy, completeness, and duplication.

- ❑ *Step 3*– If the TF was written against an application that is supported by CUBIC, the document and software findings discovered in test can be cross referenced to a PR/CR or DRR at the application PM's direction.

- ❑ *Step 4* – Prior to the next test of the application, all open TFs are reviewed and statuses are updated, as necessary.

- ❑ *Step5* – During the next test, the previously identified TFs are validated to ensure implementation. If the TFs have been implemented, they are closed by the testing organization. Any new findings are submitted. At this point, the process starts again.

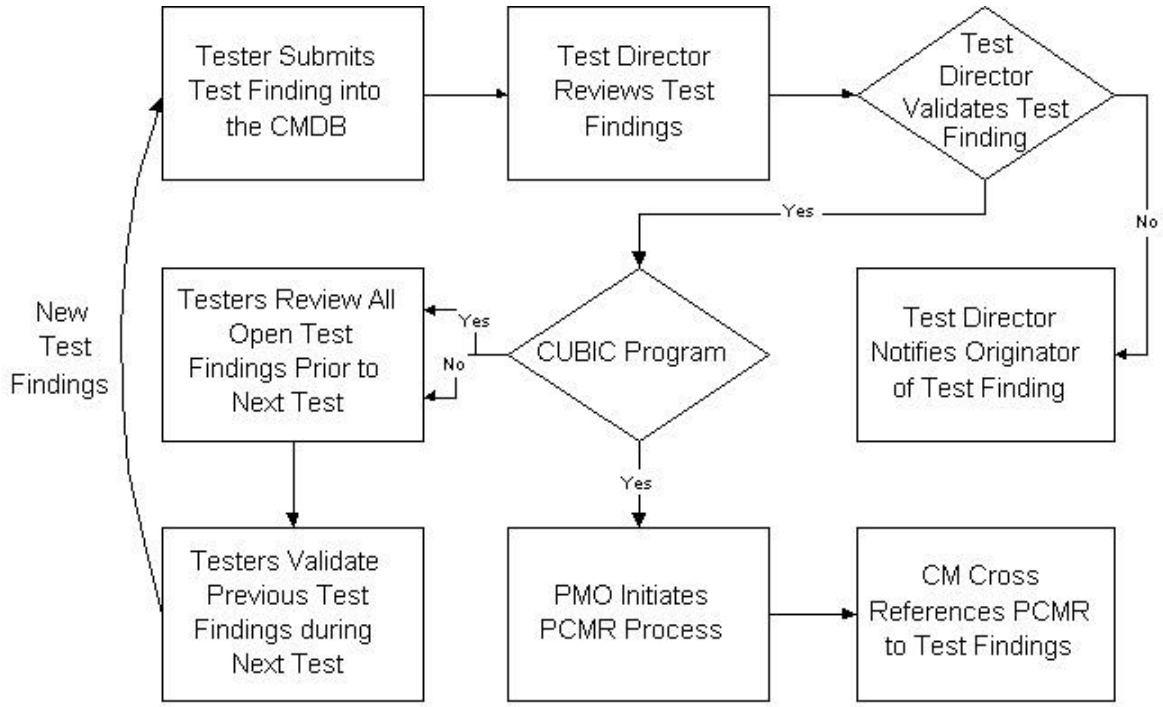
3.3 IMPACT CODE DESCRIPTIONS

3.3.1 JITF

The following defines the four (4) types of impact codes used by the JITF:

- ❑ *Impact Code 1* - A finding that, without resolution, either
  a) prevents the application from proceeding further in testing or operation;

Exhibit 3-1. Test Finding Process



b) prevents the application from proceeding further in testing or operation;
c) prevents either the application or another application or component of the infrastructure from operating properly;
d) creates a security vulnerability in the mission application or site architecture that can be exploited by a general user without taking advantage of other vulnerabilities or capabilities; or
e) **excessively** increases the level of effort of site personnel to install, manage, or use the mission application or other applications.

An Impact 1 finding is given if no workaround is available during the testing period, or if the resolution requires an excessive level of effort on the part of the mission application developer and (possibly) other agents to implement, validate, and incorporate into the mission application baseline.

For findings that clearly have no workaround, the level of effort is a key determinant for Impact 1 findings. The time or expertise required to install, manage, or use the application must be well beyond what is reasonably expected for an IMA - e.g., if the installation guide says that the IMA can be installed in a single day, but the installation takes several days, then an Impact 1 can be appropriately applied.

- *Impact Code 2* - A finding that, without resolution,
  a) has a significant effect on the operation of either the application or on another application or component of the infrastructure; or
  b) creates a security vulnerability in the application or site architecture

that could be exploited by a general user only if the user is able to take advantage of other vulnerabilities or capabilities not typically available to him or her.

The finding can be temporarily resolved by a workaround that is implemented as a change in procedure or configuration. The successful implementation of the workaround requires technical expertise that is not expected of general users, or the workaround requires a significant level of effort by site administrators. The workaround does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF.

Impact 2 findings may cause integration test failures depending upon the level of effort required to implement workaround (and confidence in it). An Impact 2 problem may be elevated to an Impact 1 if proposed workarounds either do not work successfully or produce additional Impact 2 and 3 findings.

- *Impact Code 3* - A finding, that without resolution has a significant effect on the operation of either the application or on another application or component of the infrastructure. The finding can be temporarily resolved by a workaround that is implemented as a change in procedure or configuration. The successful implementation of the workaround does not require technical expertise that is not expected of general users, or the workaround does not require a significant level of effort by site administrators. The workaround does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF.

Impact 3 findings generally do not cause integration test failure unless the number of findings increases the level of concern about the overall quality of the application.

- *Impact Code 4* - A finding that does not prevent the application from proceeding further in its testing or does not significantly affect the operation of the application or another application or component of the infrastructure. The finding can be resolved by a workaround that can be implemented as a change in procedure or configuration during integration testing without a significant level of effort, or the finding can be left as is. Even though the finding has some affect on the configuration or operation of the application or of other components of the site architecture, the general user will be able to perform mission functions, and the administrator will be able to manage the application. Findings in this category are of lesser importance, but the accumulation of Impact 4 findings may result in an overall finding at a higher Impact level.

3.3.2 SECURITY

TFs generated during security testing use four (4) Category codes. Any security test finding that identifies a vulnerability to the system is considered classified.

The following defines the definition for security testing impact codes or Category Codes:

- Security Category Code I - A significant security finding which must be fixed prior to operational use.

- Security Category Code II - A security related finding which must be fixed

within a specific time period in order for approval to be granted.

- ❑ Security Category Code III - A security relevant recommendation for which implementation is optional.

- ❑ Security Category Code IV - A non-security relevant recommendation for which implementation is optional.

SECTION FOUR
PROBLEM REPORT/CHANGE REQUEST/MULTIPLE APPLICATION PROBLEM/REQUIREMENT (PCMR) PROCESS

4.1 PCMR OVERVIEW

The objective of the PCMR process is to provide a methodology based upon sound engineering principles that will close the user-developer communications gap, place software development control firmly in the hands of the procuring agency, and produce computer software products that are acceptable in the eyes of the user. The PCMR engineering management process fully encompasses all software development functions from requirements definition through test and integration.

4.2 CM RESPONSIBILITIES

CM is the central repository for all PCMRs submitted against supported applications' software. Once the software baseline has completed the approval process, all software problems and proposed changes will be submitted, evaluated, approved or disapproved, implemented, verified, and released according to these PCMR procedures. This scheme will ensure that the configuration identification for the software is current and that no unauthorized changes are incorporated.

PRs will be used to record discrepancies found in the operational software. CRs will be used to request changes and/or enhancements to the operational baseline. MAPs will be used for PRs/CRs that affect multiple CM-supported applications or CM supported applications and other DODIIS applications, non-DODIIS, and COTS products. CM provides the program CCB and CCCB with information necessary for the decision making process. This process ensures that changes to the application are controlled and PMOs and users know the costs and benefits.

The MAP process enhances interoperability by maintaining interfaces, as defined in Interface Control Documents (ICDs), between supported programs, and coordinating advances in infrastructure support products. The process also provides a unified voice for the intelligence community to address problems and required changes to COTS products, ensuring that commercial vendors appreciate the impact to the complete customer base.

ICDs are required documents under the IMA Certification Process. An ICD Data Item

Description (DID) was initially approved for CUBIC and can be used as a guideline for PMOs requiring ICDs. A copy of the DID can be obtained from CM.

Requirements are information maintained by CM to track program level requirements for future versions. These requirements translate into program specifications. When requirements are maintained by CM in the CMDB, PRs and CRs can be cross-referenced back to these baseline requirements.

4.3 PCMR PROCESS

The PCMR process, as illustrated in Exhibit 4-1, starts and ends with the user and involves the entire user community. The procedure for processing PCMRs provides coordination between all of the players, ensuring that user requirements are not lost and are properly implemented. The steps to this process are described in the following paragraphs.

- *Step 1* - A software finding can be submitted by a site, PMO, executive manager, or the development contractor by using the software input form in the CMDB at any time during the life cycle of the program. Users who do not have Internet/Intelink access can use E-mail, message traffic via the AUTODIN communications network, facsimile, or regular mail. If the finding is classified, the user must submit it by using the CMDB software input form on Intelink or other appropriate means for transmitting classified information. If the finding is an Impact Code 1, follow the procedures outlined in Section 4.3.3. Impact Code descriptions are detailed in Section 4.3.1.

- *Step 2* - All findings are sent to the PMO for evaluation. CM will verify that all necessary information has been included in the form or message and that the problem exists in a currently approved baseline.

  If additional information is needed, the originator is contacted to request further details or clarification of the problem or new requirement. Notification is sent to the originator to verify that the finding has been received. To eliminate duplication and time-consuming evaluation, sites should review PCMRs before submitting a new finding. A site that is experiencing the same problem submitted by another site should add a concurrence message via the Notebook option in the CMDB to the PCMR, referencing any additional information regarding the problem they are experiencing at their site. Concurrence messages play a significant role for successful software maintenance efforts on any PCMR. This provides the PMO and other users with essential information on the scope and criticality of the problem or requested change.

- *Step 3* - The PMO will verify the finding by reproducing the problem on the program's current baseline or through analysis. This verification is performed/directed by the PMO engineer and could be performed anywhere the baseline exists other than the originating site. Information identified during the verification activity can be forwarded to the developer to assist in the creation of a workplan. If the finding is disapproved, the originator and any other pertinent agencies will be

notified via the CMDB. Valid findings will be examined to determine that the impact code is correct and to verify that the finding does not duplicate work already in progress. Duplicate findings will reference the PR already being worked. If additional information is provided in the duplicate finding that will assist in the correction of the original PR, it will be noted. The same action will take place with any concurrence messages from other sites. CRs will be evaluated and approved or disapproved by the PMO upon coordination with the executive manager and program CCB procedures. These valid findings will be made official PR/CRs in the CMDB. The PMO will determine if the PR/CR affects another application; if it does a MAP will be initiated.

- *Step 4* - The PMO will determine if a workplan should be requested from the development contractor. A workplan outlines the estimated time, cost, schedule, design approach to implement an approved PCMR. It also includes a history of all affected software modules and documents. This ensures that the costs and benefits of problem fixes and enhancements to the application are known by program management and are considered when determining changes to software baselines.

  Requesting a workplan from the development contractor is accomplished via a notification letter, as seen in Exhibit 4-3, generated by CM upon direction of the PMO. All workplans are stored and maintained by CM using the CMDB.

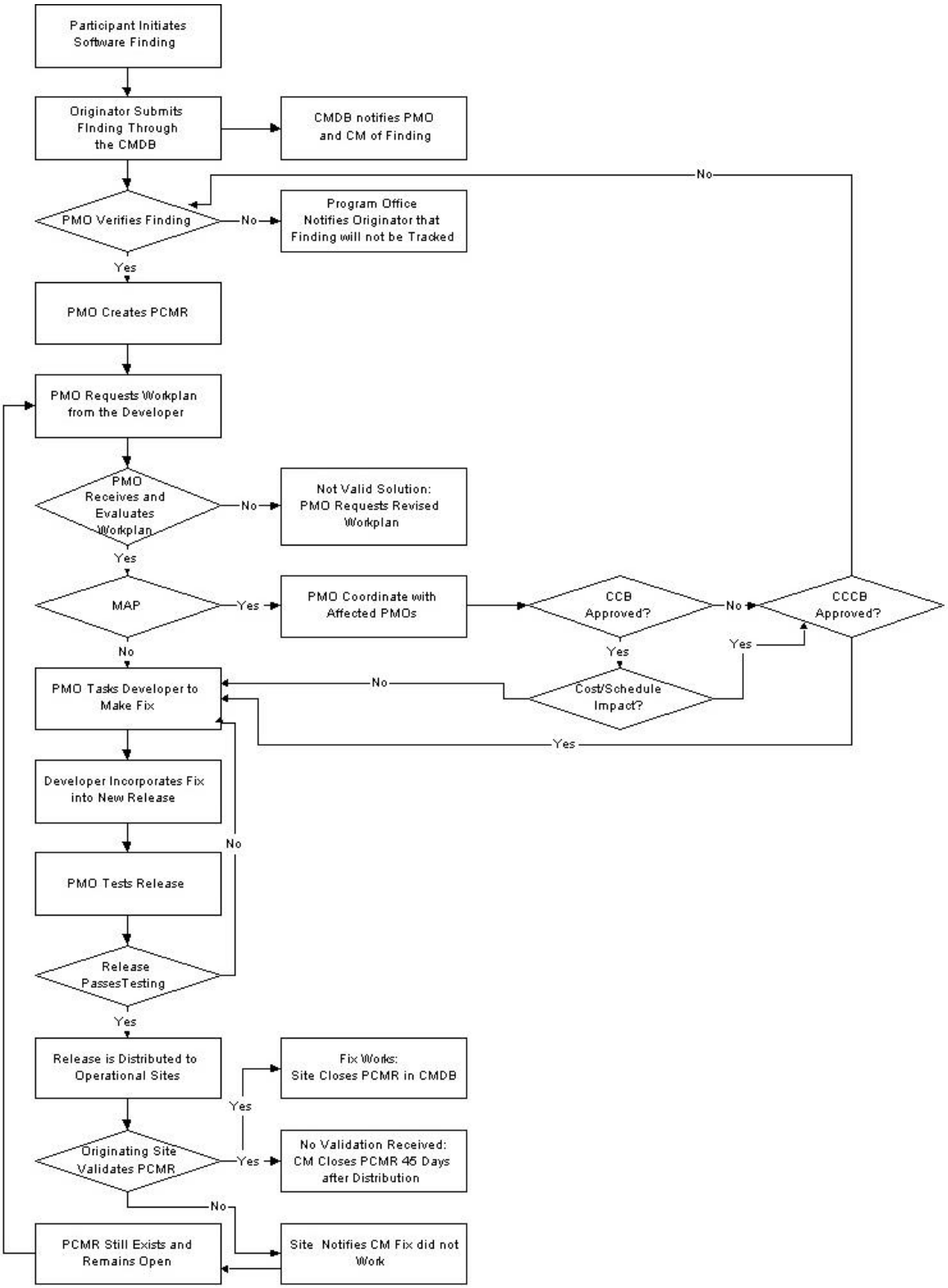
- *Step 5* - If upon developer's review the problem is valid and the change will affect other programs, a MAP record will be entered and all affected PMOs will be notified. PMOs will review the MAP and provide an impact analysis or workplan.

- *Step 6* - The development contractor submits the workplan via the CMDB to the PMO for review within 14 days of receipt of the notification letter. The amount of time the development contractor has to submit a workplan is often specified in the contract. The 14 days is to be used as a guideline. The PMO, coordinating with the executive manager, may decide upon review of the workplan to discontinue the effort based upon a variety of factors, e.g., funding or time constraints and situations overtaken by other events, etc. If this occurs, the PCMR will be closed and all pertinent agencies will be notified. If the workplan is not a valid solution, a revised workplan will be requested or the PCMR will be re-evaluated by the PMO and, depending upon the circumstances, could be closed.

- *Step 7* - Once the workplan has been approved by the PMO, the development contractor is then directed via a tasking letter sent by CM, as seen in Exhibit 4-4, to implement the change as described.

  For MAPS: CM coordinates the MAP process with the PMOs, ensuring that all information is collected and presented at the next scheduled program CCB.

Exhibit 4-1. PCMR Process



The program CCB reviews and approves or disapproves the MAP package. If approved and there are no cost and schedule impacts, the executive manager, in coordination with the PMO, determine the implementation strategy. If approved and there are cost and schedule impacts the MAP package is forwarded to the CCCB.

The CCCB approves or disapproves the MAP. If approved, the change is implemented as prescribed by the MAP package for each affected application. Disapproved MAPs are closed by CM or re-evaluated by repeating the MAP process. A MAP may require coordination by the CCCB with CCBs outside the programs supported by CUBIC prior to approval or disapproval of the requested change.

Based on the complexity of the MAP, the PMO may want to coordinate an Interface Control Working Group (ICWG) comprised of members from the affected programs to assist in working out the MAP issues.

- *Step 8* - The development contractor completes the change and incorporates it into the next release.

- *Step 9* - The release is tested.

- *Step 10* - The approved release is then distributed to the sites along with a SVD and other application documentation as required. The sites are then responsible for referencing the SVD and verifying any PR/CR listed as originating from their site and ensuring it has been incorporated. The sites need to update the status, fixed or problem still exists, in the CMDB within 45 days of the release with their responses.

- *Step 11* - If no validation information is provided by the site after 45 days, the PRs/CRs listed in the SVD will be closed by CM upon direction of the PMO and notification will be sent to the pertinent agencies. Sites can request that the 45 day deadline be extended or the PMO can designate an alternate timeframe.

- *Step 12* - If the PR/CR was not implemented as stated in the SVD, the PR/CR remains open. At this point the cycle begins again at Step 4.

4.3.1 IMPACT CODE DESCRIPTIONS

The following paragraphs define the five (5) types of impact codes and to what situations they apply:

- *Impact Code 1*
  a) Prevents the accomplishment of an essential capability.
  b) Jeopardizes safety, security, or other requirement designated "critical".
  Impact Code 1 problem reports are considered classified. See Section 4.3.3 on how to enter an Impact 1 PR.

- *Impact Code 2*
  a) Adversely affects the accomplishment of an essential capability and no work around solution is known.
  b) Adversely affects technical, cost, or schedule risks to the project or to life cycle support of the system, and no work-around solution is known.

- *Impact Code 3*
  a) Adversely affects the accomplishment of an essential capability but a work-around solution is known.
  b) Adversely affects technical, cost, or schedule risks to the project or to life cycle support of the system, but a work-around solution is known.

- *Impact Code 4*
  a) Results in user/operator inconvenience or annoyance but does not affect a required operational or mission-essential capability.
  b) Result in inconvenience or annoyance for development or maintenance personnel but does not prevent the accomplishment of the responsibilities of those personnel.

- *Impact Code 5*
  Any other effect.

4.3.2 CLASSIFICATION ISSUES

If a submitted PR or CR is classified then it must be handled accordingly. For security reasons, classified PRs/CRs will be maintained on the CMDB Intelink server. The only information that is guaranteed to be unclassified, and will be maintained on the CMDB Internet server, is the PCMR number, date, type, impact code, base release number, originator name, phone, and status. A program engineer or manager will check the title and, if unclassified, it can be entered. An unclassified title will be selected for entry into the CMDB by the engineer or manager if the original title is classified.

4.3.3 SUBMISSION OF AN IMPACT CODE 1 PR

The following paragraphs describe the steps necessary in the life cycle of an Impact Code 1 PR. The process is illustrated in Exhibit 4-2.

- *Step 1* - The Impact Code 1 is identified from the originating site.

- *Step 2* - The site notifies the PMO via telephone stating that a Code 1 problem exists.

- *Step 3* - The site enters the finding into the CMDB on Intelink.

- *Step 4* - The PMO evaluates the problem to make a determination if the PR is an Impact Code 1 with coordination of the executive manager.

- *Step 5* - If the PR is an Impact Code 1, the process will proceed to step 6. If it is not an Impact Code 1, it will be downgraded and the site will be notified by the PMO with the reason for the downgrade. The PR will progress from this point via normal PR work flow channels.

- *Step 6* - The PMO, or their representative, coordinates with the development contractor via phone or other immediate way of communication and requests work to begin on the fix, with precautions taken due to the classification of the issue.

- *Step 7* - The development contractor works the fix in coordination with the PMO and implements the fix at the affected site.

- *Step 8* - The originating site determines whether the fix resolves the problem and updates the CMDB with the results. If the fix resolved the problem, the process proceeds to step 9. If the fix did not resolve the problem, the PMO notifies the development contractor of the updated status and they rework the problem, as necessary.

- *Step 9* - The PMO will notify the development contractor and update the status.

- *Step 10* - The development contractor distributes the fix to other affected sites and baselines the fix in the next software release.

4.4 SUMMARY

The PCMR procedure ensures the coordinated participation of all interested members of the organization throughout the software development process. User requirements are identified and, through the detailed procedures, are tracked and monitored by CM using the CMDB. This approach reduces technical, schedule, and cost risks.

All contributors to the program, e.g., Government representatives, contractors, both development and IV&V, and operational sites, should meet semi-annually to review the status and disposition of all open CM records. This activity ensures that status accounting information remains accurate and current.

Exhibit 4-2. Impact Code 1 Process

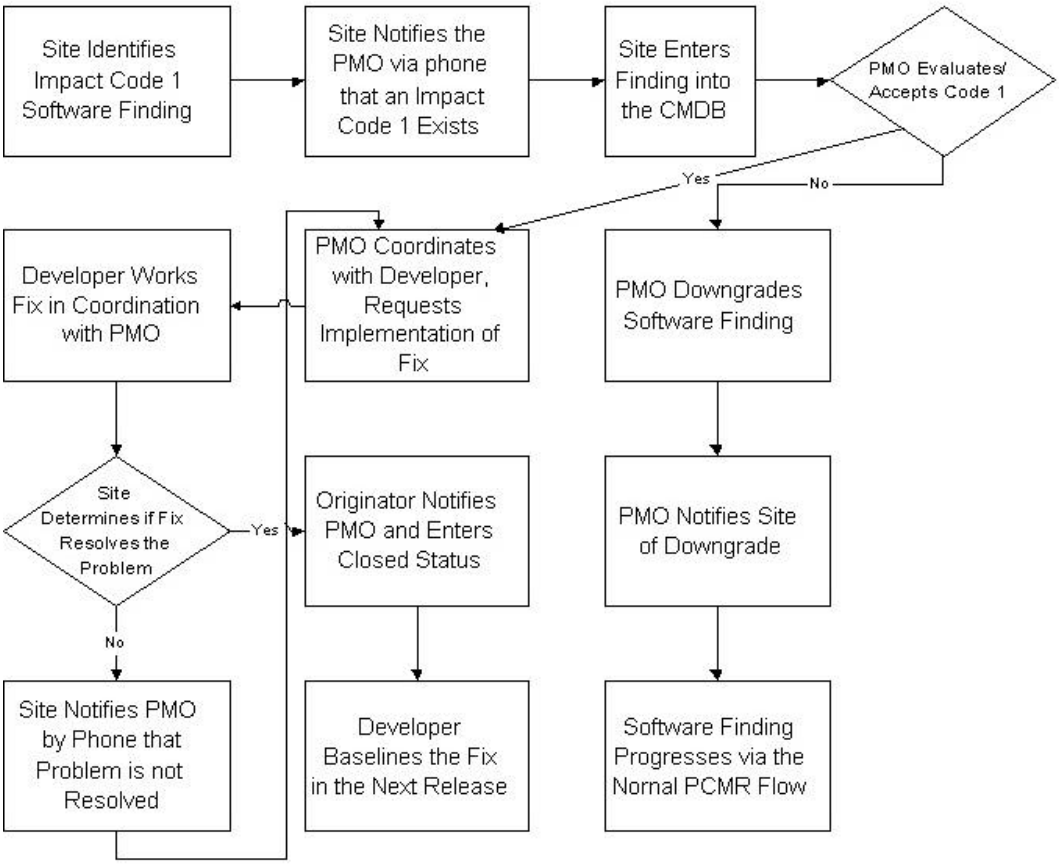


Exhibit 4-3. Sample Notification Letter

AFRL/IFEB
32 Brooks Road
Rome NY 13441-4114

Jane Doe
Company Name
Street Address
City, State Zip Code

Dear Ms. Doe,

This is a Problem Report/Change Request Notification Letter, Contract F00000-00-0-0000. For the attached Change Requests (CRs) or Problem Reports (PRs), please take action to determine impact on application baseline, estimated number of hours to solve the problems, estimated completion dates, a design approach, estimated cost, software and documentation affected. Notify AFRL/IFEB by letter of your evaluations within 10 days of receipt of this letter.

This letter is not to be construed as an order under the contract. Changes involving increases or decreases in prices, the delivery schedule, or other contract terms and conditions which may form the basis of claims against the Government will be directed only by the contracting officer.

This request should not be construed as authorization to exceed the funded contract ceiling for Software Problem Report resolution. Please advise this office immediately if any of the above items could require additional funding to complete.

This is a coordinated executive manager and AFRL/IFEB letter. AFRL/IFEB POC is John Doe, DSN 587-0000, Commercial (315) 330-0000.

Sincerely

John Doe
Air Force Research Laboratory
Program Manager

Attachments:
1. List of PRs/CRs dtd DD MM YY
2. PR/CR Pkg #

cc:
Executive Manager

AFRL/IFE Program
AFRL/IFEB CM

Exhibit 4-4. Sample Tasking Letter

Air Force Research Laboratory/IFEB
32 Brooks Road
Rome NY 13441-4114

Jane Doe
Company Name
Street Address
City, State Zip Code

Dear Ms. Doe,

Problem Report/Change Request Tasking Letter, Contract F00000-00-0-0000. Request you implement the recommended solutions as outlined in your Problem Report (PR) and/or Change Request (CR) workplans for the attached list of PRs/CRs.

All previous tasking letters are null and void.

This letter is not to be construed as an order under the contract. Changes involving increases or decreases in prices, the delivery schedule, or other contract terms and conditions which may form the basis of claims against the Government will be directed only by the contracting officer.

This request should not be construed as authorization to exceed the funded contract ceiling for Software Problem Report resolution. Please advise this office immediately if any of the above items could require additional funding to complete.

This is a coordinated executive manager and AFRL/IFEB letter. AFRL/IFEB POC is John Doe, DSN 587-0000, Commercial (315) 330-0000.

Sincerely

John Doe
Air Force Research Laboratory
Program Manager

Attachments:
1. List of PRs/CRs dtd DD MM YY
2. PR/CR Pkg #

cc:
Executive Manager
AFRL/IFE Program
AFRL/IFEB CM

SECTION FIVE
DOCUMENT MANAGEMENT PROCESS

5.1 DRR OVERVIEW

DRRs are a tool used within a program to evaluate, verify, and approve or disapprove the accuracy and adherence to standards for documentation releases. The document review process, as illustrated in Exhibit 5-1, ensures that all DRRs are implemented according to established CM procedures.

5.2 DRR PROCESS

- *Step 1*- The developer submits the documentation in draft form to CM via the PMO.
- *Step 2* - CM logs the documentation into the CMDB technical library, compiles any old DRRs that may have been written against the previous version of the document, and notifies appropriate technical personnel of the receipt of the revised documentation and the existence of any old DRRs.
- *Step 3* - Technical document review is coordinated by the PMO. Document reviews are generally initiated by QA personnel within the PMO, the development contractor, and/or any other requested reviewers. Specific users may be asked to comment on documents as well. Each review group has a designated DRR coordinator.
- *Step 4* - The reviewers assure that any old DRRs written against a previous version of the document have been incorporated, as well as writing up any new errors.
- *Step 5* - After all the comments are documented by the review group, they are submitted to the DRR coordinator who reviews them for completeness and duplicate comments. The coordinator then assigns an alternate ID (identification) number and enters the DRRs into the CMDB using the document input form in the CMDB. If the DRR is classified, the DRR must be submitted through the input form of the CMDB on Intelink. If a submitter does not have access to the database, hardcopies will be accepted.
- *Step 6* - CM initiates a transmittal letter upon direction of the PMO. An illustration of a DRR transmittal letter can be seen in Exhibit 5-2.

- *Step 7* - The development contractor reviews the comments and reworks the documentation as necessary before submitting a revised edition back to the PMO. The development contractor can utilize change bars when revising documentation to allow the reader to see what information has been updated.

- *Step 8* - Developers respond to the comments by entering a status and disposition in each DRR record.

- *Step 9* - PMO and any other original reviewers, if possible, review the revised documents along with the developer's disposition comments and decide whether the DRR has been satisfied. The PMO, depending upon the developer's comments, may close, withdraw, or hold the DRR open. Those held open will remain so until further documentation revision is forwarded by the developer and the DRR is deemed rectified by a Government reviewer. Disputes over Government validated DRRs must be resolved by the developer with the PMO prior to the release of the revised documentation.

  If the PMO does not approve the revised document, the open DRRs are returned to the developer and Step 7 begins again.

- *Step 10* - Approved documentation is then designated for distribution as required to the operational sites.

5.3 CDRL TRACKING PROCEDURES

CDRLs define the type and frequency of required data items. CDRL tracking procedures help monitor development of the software and its associated documentation. The PMO and/or the Contracting Officer's Technical Representative (COTR) approves and tracks all data items required by the program/application.

The PMO needs to know when a newly-generated document requires authentication or someone proposes a change to an existing authenticated document. The PMO schedules and monitors a full review of the new or changed document in accordance with DRR procedures. This review cycle may also be set by contract and is defined in the CDRL.

For documents needing revision, the PMO notifies the development contractor as prescribed by the contract. With coordination, CM can assure that all the necessary CDRL tracking data, including contract, distribution, deliverables, review schedules, library entries, and DRRs are entered into the CMDB. Once this information is included in this database, all interested Government and contractor personnel can access it.

The CM library maintains information on, and copies of, CDRL documents approved by the Government. The library distributes documents as requested by the PMO. Library services, the DRR process and CDRL tracking provide complete life cycle management for all program documentation.

Exhibit 5-1. Document Review Report Process

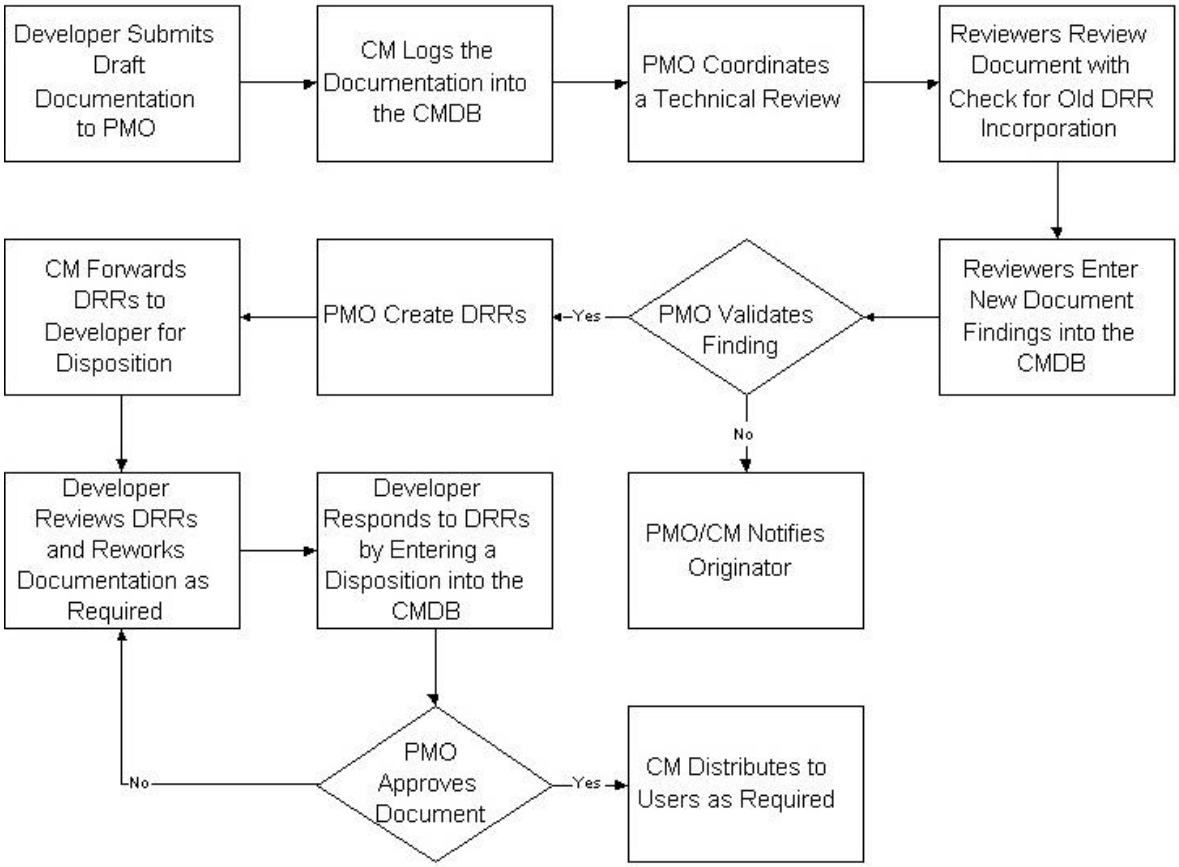


Exhibit 5-2. Sample DRR Transmittal Letter

Air Force Research Laboratory/IFEB
32 Brooks Road
Rome NY 13441-4114

Ms. Jane Doe
Company
Street Address
City, State Zip Code

Dear Ms. Doe:

Enclosed is a summation report of Document Review Reports (DRRs) written against the documentation identified in the attached report for contract F30602-00-0-0000.

This letter is not to be construed as an order under the contract. Changes involving increases or decreases in prices, the delivery schedule, or other contract terms and conditions which may form the basis of claims against the Government will be directed only by the contracting officer.

This request should not be construed as authorization to exceed the funded contract ceiling for CUBIC document updates. Please advise this office immediately if any of the above items could require additional funding to complete.

This is a coordinated executive manager and AFRL/IFEB letter. AFRL/IFEB POC is John Doe, DSN 587-0000, Commercial (315) 330-0000.

Sincerely

John Doe
Air Force Research Laboratory
Program Manager

Attachments:
1. Summation Report 1 March 1999

cc:
Executive Manager
AFRL/IFE Program
AFRL/IFEB CM

SECTION SIX
ACTION ITEM PROCESS

6.1 AI OVERVIEW

AIs are a management tool used by the PMO and executive manager to identify and track issues for the program. AIs may be initiated at user group meetings, reviews, or other technical exchange meetings. They may be initiated by any participant in the software development process and are tracked by CM to solution/closure. The process is illustrated in Exhibit 6-1.

6.2 AI PROCESS

- *Step 1* - The AI is initiated by a participant of the program at any time during the life cycle of the program. The assignee of the AI takes responsibility for completing the AI.

- *Step 2* - The AI is entered into the CMDB.

  For AIs generated outside of a PMO attended meeting: The user submits an AI through the input form of the CMDB. If the AI is classified, the user must submit the AI through the action input form of the CMDB on Intelink. Users who do not have Internet/Intelink access can use E-mail, message traffic via the AUTODIN communications network, facsimile, or regular mail. All AIs will be sent to the PMO for screening and evaluation. CM will verify that all necessary information has been included in the form or message.

  If additional information is needed, the originator is contacted to request further details or clarification.

- *Step 3* - Once the AI is validated, the CMDB will notify the originator and assignee via automatic notification.

- *Step 4* - The assignee will perform the action needed and update the status and disposition in the CMDB.

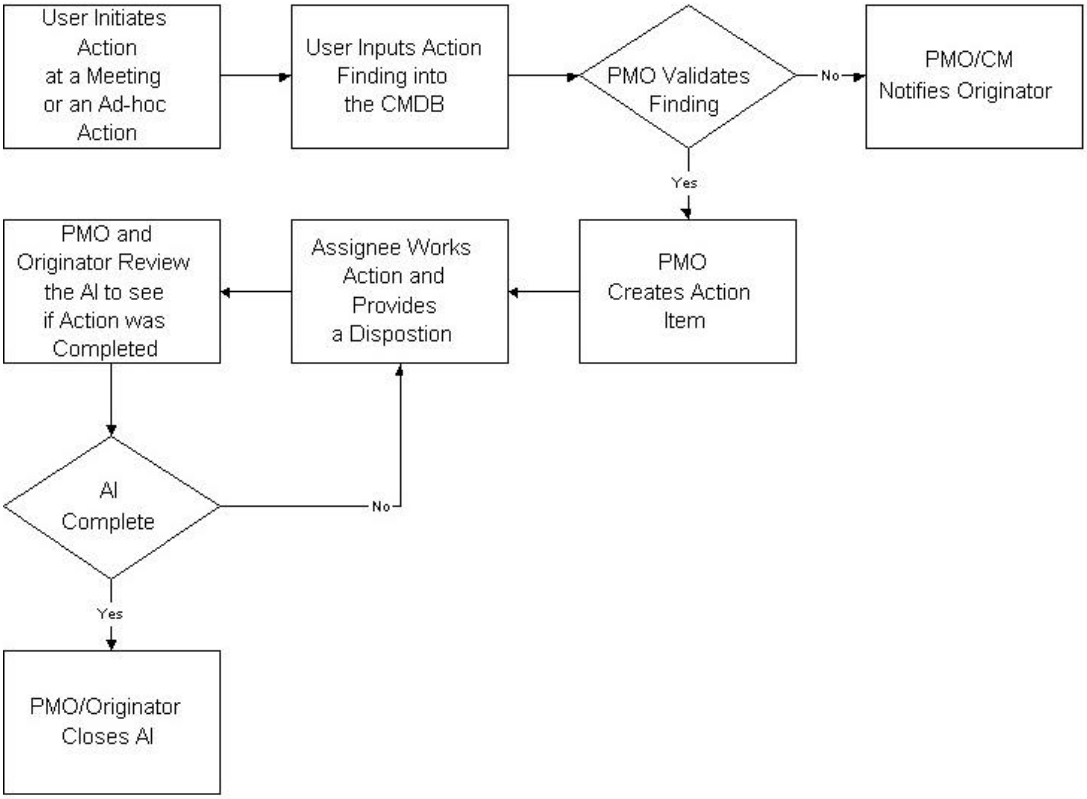
  Suspense dates on AIs are periodically checked. If an AI is overdue, notification will be sent to the PMO, originator, and assignee for review.

- *Step 5* - The PMO and originator will review the AI to determine if the action was performed satisfactorily.

- *Step 6* - If the AI was performed satisfactorily, the originator and

PMO will close the AI. If not, Step 4 begins again.

Exhibit 6-1. Action Item Process



SECTION SEVEN
SOFTWARE RELEASES

7.1 SOFTWARE RELEASES

A software release is the distribution of the latest baselined version of an application. Software release information is tracked in the CMDB for all supported programs. This allows the Government to track who has the software and any COTS software distributed with a release. The information is obtained from various sources, including but not limited to the SVD, PMO, E-mail from sites, and information obtained from the development contractor. The purpose of the Release section of the CMDB is to provide a consolidated location for information on software versions.

7.1.1 PMO RESPONSIBILITIES

The PMOs have the responsibility to:

- ❑ Provide a schedule for the release including anticipated test and distribution dates.
- ❑ Provide a list of sites and users that will receive the release.
- ❑ Provide a list of documents to be included in the release package, including identification of those documents distributed to the field.

7.1.2 SITE RESPONSIBILITIES

The sites have the responsibility to:

- ❑ Maintain a Profile on the CMDB to ensure any changes to pertinent information are reflected in a timely manner.
- ❑ Notify CM if their site is leaving or joining the program software community.
- ❑ Provide in a timely manner a current mailing address for the distribution of the release when requested by CM.
- ❑ Return the receipt acknowledgment letter provided in each software and/or documentation release package(s) via mail, facsimile, or automated form on the CM homepage.
- ❑ Provide CM the installation date and any installation details immediately following installation of all software releases via Library Audit in the CMDB. Users who do not have Internet/Intelink access can use E-mail, phone, or message traffic.

- Provide estimated installation date and explanation for any delay if the site is not planning on installing within 30 days.
- Verify incorporation of PRs/CRs into the release and update the status of those PRs/CRs that are now fixed or are still valid in the CMDB.

7.1.3 CM RESPONSIBILITIES

CM has the responsibility to:

- Input site information obtained from a data call into the CMDB.
- Notify PMOs of changes to site profile information as required.
- Reproduce the software release and appropriate documentation.
- Distribute the software release and appropriate documentation to the PMO specified sites.
- Maintain the distribution lists on which sites received the software release in the CMDB.
- Upon receipt of the acknowledgment letter provided in each software and/or documentation release package(s), update the CMDB with the appropriate information.
- Coordinate user requests with PMOs.

7.1.4 DEVELOPMENT CONTRACTOR RESPONSIBILITIES

The development contractor has the responsibility to:

- Notify CM of any changes or updates to user/site information based upon data provided by site representatives, help desk activities, or other methods.
- Review CM user site information prior to distribution of any software release directly from the developer's site to ensure correct mailing addresses and POC information.
- Notify CM of distribution software releases made by the developer per contracted requirement. All information to maintain the release records can be submitted via softcopy or hardcopy.

7.2 EMERGENCY RELEASES

Emergency releases will be used to effect repairs to baselined versions or revisions that are not capable of operating due to Impact Code 1 problems as described in Section 4. These problems affect either the overall operational capability or severely compromise national security. The PMO and executive manager will coordinate emergency releases. Any changes will be fully documented and incorporated into the next scheduled release of the software. Patch numbers, distribution, and installation information must be reported to CM as soon as possible for tracking purposes and easy identification of those sites, which are above the current approved baseline.

APPENDIX A

ACRONYMS

ADM	Acquisition Decision Memorandum
AF	Air Force
AFRL	Air Force Research Laboratory
AI	Action Item
AIG	Address Indicator Group
AUTODIN	Automatic Digital Network
CCB	Configuration Control Board
CCCB	CUBIC Configuration Control Board
CDRL	Contract Data Requirements List
CI	Configuration Item
CM	Configuration Management
CMDB	Configuration Management Database
COTR	Contracting Officer's Technical Representative
COTS	Commercial Off The Shelf
CR	Change Request
CRR	Certification Readiness Review
CUBIC	Common User Baseline for the Intelligence Community
DAWS	Defense Automated Warning System
DD	Defense Document
DEV	Deviation
DEXA	DODIIS Executive Agent
DID	Data Item Description
DMB	DODIIS Management Board
DMS	Defense Messaging System
DOC	Document
DOD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DRR	Document Review Report

DSN	Defense Security Network
ECP	Engineering Change Proposal
EIA	Electronic Industries Association
ESC	Electronic Systems Center
GOTS	Government Off The Shelf
GITC	General Intelligence Training Council
ICD	Interface Control Document
ICWG	Interface Control Working Group
ID	Identification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFEB	Integration and Interoperability Branch
IMA	Intelligence Mission Application
ISO	International Organization for Standardization
IV&V	Independent Verification & Validation
JITC	Joint Interoperability Test Command
JITF	Joint Integration Test Facility
MAIS	Major Automated Information System
MAP	Multiple Application Problem
MAXI	Modular Architecture for Exchange of Information
MB	Megabyte
MDA	Milestone Decision Authority
MDAP	Major Defense Acquisition Program
P^3I	Pre-Planned Product Improvement
PLA	Plain Language Address
PM	Program Manager

PMO	Program Management Office
PMP	Program Management Plan
POC	Point of Contact
PR	Problem Report
QA	Quality Assurance
RFC	Request for Change
SCI	Sensitive Compartmented Information
SETA	System Engineering and Technical Assistance
SPR	Software Problem Report
SVD	Software Version Description
SW	Software
TEMS	Technical and Engineering Management Support
TF	Test Finding
U&S	Unified and Specified
WAV	Waiver