ARMY, MARINE CORPS, NAVY, AIR FORCE

AIR LAND SEA APPLICATION CENTER

JTF IM

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR JOINT TASK FORCE INFORMATION MANAGEMENT

FM 6-02.85 (FM 101-4)
MCRP 3-40.2A
NTTP 3-13.1.16
AFTTP(I) 3-2.22

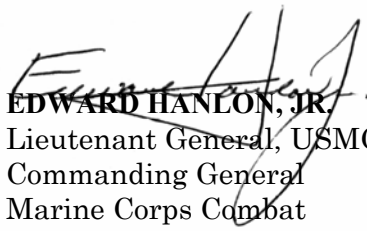
SEPTEMBER 2003

MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES

FOREWORD

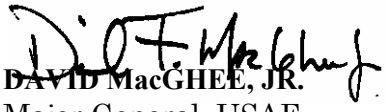
This publication has been prepared under our direction for use by our respective commands and other commands as appropriate.

DAVID A. FASTABEND
Brigadier General, U.S. Army
Deputy Chief of Staff for
Doctrine, Concepts and Strategy
U.S. Army Training and Doctrine
Command



EDWARD HANLON, JR.
Lieutenant General, USMC
Commanding General
Marine Corps Combat
Development Command

R. A. ROUTE
Rear Admiral, USN
Commander
Navy Warfare Development
Command



DAVID MacGHEE, JR.
Major General, USAF
Commander
Headquarters Air Force
Doctrine Center

This publication is available at Army Knowledge Online (www.us.army.mil) and at the General Dennis J. Reimer Training and Doctrine Digital Library (www.adtdl.army.mil).

PREFACE

1. Scope

This publication provides multi-Service tactics, techniques and procedures (MTTP) for establishing an organized and disciplined approach for information management (IM) at the joint task force (JTF). It provides a "scheme of maneuver" for managing information. This publication provides a variety of options the JTF headquarters (HQ) information management officer (IMO) may use in developing a JTF information management plan (IMP).

2. Purpose

This publication provides the JTF tactics, techniques, and procedures (TTP) for effective and efficient distribution, control, and protection of information. It provides TTP for filtering, fusing, and prioritizing information, thereby enabling the commander to anticipate changing battlespace conditions, establish priorities, and facilitate decisionmaking.

3. Applicability

The audience for this publication includes commanders, staffs, and agencies at all levels within and supporting a JTF. This publication can serve as a source document for developing joint and service manuals, publications, and curricula or as a stand-alone document at the JTF and component levels. Furthermore, this publication enhances the 2.0, 3.0, 5.0, and 6.0 series of Joint Publications, providing insight into the procedures for effective and efficient management of information. While written to a JTF level audience, this publication applies to any organization concerned with improving the flow and quality of information.

4. Implementation Plan

Participating Service command offices of primary responsibility (OPRs) will review this publication, validate the information, reference, and incorporate it in Service and command manuals, regulations, and curricula as follows:

Army. Upon approval and authentication, this publication incorporates the procedures contained herein into the US Army Doctrine and Training Literature Program as directed by the Commander, US Army Training and Doctrine Command (TRADOC).Distribution is in accordance with Initial Distribution Number (IDN) 115770.

Marine Corps. The Marine Corps will incorporate the procedures in this publication in U.S. Marine Corps training and doctrine publications as directed by the Commanding General, U.S. Marine Corps Combat Development Command (MCCDC). Distribution is in accordance with the Marine Corps Publication Distribution System.

Marine Corps PCN 144 000057 00

Navy. The Navy will incorporate these procedures in U.S. Navy training and doctrine publications as directed by the Commander, Navy Warfare Development Command (NWDC). Distribution is in accordance with Military Standard Requisition and Issue Procedure Desk Guide (MILSTRIP Desk Guide) and Navy Standing Operating Procedure Publication 409 (NAV SOP Pub 409).

Air Force. The Air Force will incorporate the procedures in this publication in accordance with applicable governing directives. Distribution is in accordance with Air Force Instruction (AFI) 33-360.

5. User Information

a. TRADOC, MCCDC, NWDC, Headquarters AFDC, and the Air Land Sea Application (ALSA) Center developed this publication with the joint participation of the approving Service commands. ALSA will review and update this publication as necessary.

b. This publication reflects current joint and Service doctrine, command and control organizations, facilities, personnel, responsibilities, and procedures. Changes in Service protocol, appropriately reflected in joint and Service publications, will likewise be incorporated in revisions to this document.

c. Unless stated otherwise, masculine nouns and pronouns in this publication do not refer exclusively to men.

d. We encourage recommended changes for improving this publication. Key your comments to the specific page and paragraph and provide a rationale for each recommendation. Send comments and recommendations directly to—

Army

Commander
U.S. Army Training and Doctrine Command
ATTN: ATDO-A
Fort Monroe, VA 23651-5000
DSN 680-3951 COMM (757) 788-3951
E-mail: doctrine@monroe.army.mil

Marine Corps

Commanding General
U.S. Marine Corps Combat Development Command
ATTN: C42
3300 Russell Road, Suite 318A
Quantico, VA 22134-5021
DSN 278-6233/6234 COMM (703) 784-6234
E-mail: deputydirectordoctrine@mccdc.usmc.mil

Navy

Commander
Navy Warfare Development Command
ATTN: N5
686 Cushing Road
Newport, RI 02841-1207
DSN 948-1164/4189 COMM (401) 841-1164/4189
E-mail: alsapubs@nwdc.navy.mil

Air Force

HQ Air Force Doctrine Center
ATTN: DJ
204 Dodd Blvd, Suite 301
Langley AFB, VA 23665-2788
DSN 574-8091 COMM (757) 764-8091
E-mail: afdc.dj@langley.af.mil

ALSA

Director
ALSA Center
114 Andrews Street
Langley AFB, VA 23665-2785
DSN 575-0902 COMM (757) 225-0902
E-mail: alsa.director@langley.af.mil

***FM 6-02.85** (FM 101-4)
***MCRP 3-40.2A**
***NTTP 3-13.1.16**
***AFTTP(I) 3-2.22**

FM 6-02.85 (FM 101-4) — **U.S. Army Training and Doctrine Command, Fort Monroe, Virginia**

MCRP 3-40.2A — **Marine Corps Combat Development Command, Quantico, Virginia**

NTTP 3-13.1.16 — **Navy Warfare Development Command, Newport, Rhode Island**

AFTTP(I) 3-2.22 — **Headquarters Air Force Doctrine Center, Maxwell Air Force Base, Alabama**

10 September 2003

JTF IM
MULTI-SERVICE TACTICS, TECHNIQUES, AND PROCEDURES FOR JOINT TASK FORCE INFORMATION MANAGEMENT

TABLE OF CONTENTS

*This publication supersedes FM 101-4, MCRP 6-23A, NWP 3-13.1.16, and AFTTP(I) 3-2.22, 8 April 1999.

FIGURES

TABLES

EXECUTIVE SUMMARY

JTF IM

Multi-Service Tactics, Techniques, and Procedures for Joint Task Force Information Management

This publication—

- Defines and outlines information management terms and processes to include filtering, fusing, and prioritizing.
- Outlines IM responsibilities for handling, managing, preserving, and protecting information.
- Provides an overview of systems available for supporting information management.
- Provides techniques on how to manage the vast amounts of information generated by different processes and systems; for example, electronic mail, homepages, the Global Command and Control System (GCCS), official message traffic, and intelligence feeds.
- Provides TTP to manage the information flow between the joint operations center and the joint intelligence support element.
- Provides guidelines on managing the information pertaining to commander's critical information requirements (CCIR), requests for information (RFI) procedures, JTF headquarters reports, JTF briefings, and operation orders.

Overview for Information Management

Chapter 1 introduces the definition and purpose of IM. It describes how IM relates to the JTF commander's decisionmaking process. It explains the relationship between this publication and a specific JTF information management plan. The chapter describes the general characteristics of information, and information use supporting the commander's decisionmaking process. It concludes with a discussion on information flow in the JTF and defines the terms filtering, fusing, and prioritizing in the context of IM.

Duties and Responsibilities

Chapter II provides a delineation of positions/cells/sections, and their IM responsibilities. It identifies the principal managers of the IM system while providing some definition of their broad responsibilities and their relationship to the JTF staff.

Information Management Requirements, Processes, Procedures

Chapter III provides guidelines on how to best manage the information generated by E-mail, GCCS, message traffic, etc. It also provides procedures for CCIR, RFI, and techniques on the management of JTF headquarters reports, briefings, and operation orders.

Information Management Systems

Chapter IV discusses some IM systems available to the JTF staff and backup processes or systems for emergencies. The chapter concludes with options for establishing communication system priorities.

Information and Information System Protection

Chapter V describes information assurance considerations (such as the vulnerability to viruses, the levels of protection and defense, and the mechanisms that must be in place to prevent the user from short cutting or bypassing levels of protection). Information assurance also includes safeguarding information.

PROGRAM PARTICIPANTS

The following commands and agencies participated in the development and revision of this publication:

Joint

Joint Staff, J6, 6000 Joint Staff, Pentagon Room 2B865, Washington, DC 2038-6000

USCENTCOM (CCJ5-O), 7115 S Boundary Blvd, MacDill AFB, FL 33621-5101

USEUCOM (EJ5-D), Unit 30400, Box 1000, APO, AE 09128

USJFCOM, 1562 Mitscher Ave, Suite 200, Norfolk, VA 23551

USPACOM (J383), BOX 64013, Camp HM Smith, HI 96861-4013

USSOUTHCOM (SCJ5-PS), 3511 NW 91st Ave, Miami, FL 33172-1271

USSPACECOM (SPJ5X), 250 S Peterson Blvd, Suite 116, Peterson AFB, CO 80914-3130

USSTRATCOM (J512), 901 SAC Blvd, Suite 2E18, Offutt AFB, NE 68113-6500

USTRANSCOM, 508 Scott Dr, Scott AFB, IL 62225-5357

Army

HQ TRADOC (ATDO-A), Ingalls Rd, Bldg 133 Room 7, Fort Monroe, VA 23651-5000

HQ XVIII ABN Corps, Fort Bragg, NC 28307-5000

Combined Arms Doctrine Directorate, 1 Reynolds Avenue, Fort Leavenworth, KS 66027-1352

U.S. Army Signal Center and Fort Gordon, GA 30905-5000

Marine Corps

Marine Corps Combat Development Command, Joint Doctrine Branch (C427) 3300 Russell Rd, 3rd Floor, Suite 318A, Quantico, VA 22134-5021

HQ U.S. Marine Corps, Strategy and Plans Division, Room 5D 616, Washington, DC 20380-1775

Navy

Navy Warfare Development Command (N5), Newport, RI 02841-1207

CDRLANTFLT, 1562 Mitscher Ave, Suite 250, Norfolk, VA 23511-2487

Chief of Naval Operations (N512), Department of the Navy, Washington, DC 20350-2000

2nd Fleet, FPO AE 09506-6000

Air Force

HQ Air Force Doctrine Center, 155 N Twining Street, Maxwell AFB, AL 36112

AFDC/DJ, 204 Dodd Blvd, Suite 301, Langley AFB, VA 23665

HQ AFCENT, 460 Box 539, APO AE 09703

HQ USAFE/SCE, APO AE 09094

HQ 3 AF/CCEA, PSC 37 Box 1, APO AE 09459

HQ 8 AF /SC/AS, Barksdale AFB, LA 71110-2279

HQ 9 AF, 524 Shaw Drive, Shaw AFB, SC 29152-5029

AFC2ISRC/SCG, 130 Andrews Street, Suite 216, Langley AFB, VA 23665

Chapter I
INTRODUCTION TO INFORMATION MANAGEMENT

"The joint force must be able to take advantage of superior information converted to superior knowledge to achieve 'decision superiority'—better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows the force to shape the situation or react to changes and accomplish its mission."

Joint Vision 2020

1. Background

Commanders use many tools and resources—personnel, equipment, supplies, and information—to effectively carry out the mission of the joint task force (JTF). Information, however, may be the most valuable asset at the commander's disposal. The right information, at the right time, allows the commander to make critical decisions that lead to mission accomplishment. With this in mind, a JTF must manage information efficiently. This publication outlines tactics, techniques, and procedures for the JTF to manage information, and describes a JTF information management (IM) organizational structure that can direct and control the flow of information. Whether the JTF is large or small, information management is critical to the operations of the JTF.

2. Information Management and Decisionmaking

a. In military operations, a military force strives to possess better information and to use that information to make timely and more effective decisions than the enemy. A force that achieves this advantage and effectively uses it to affect enemy perceptions, attitudes, decisions, and actions has information superiority. Information superiority is the operational advantage derived from the ability to collect, process, store, disseminate, and display an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

b. Information superiority enables U.S. forces to see, understand, act first, and finish decisively. The operational advantage of information superiority allows friendly actions to influence the battlespace effectively while the adversary cannot. Commanders exploit information superiority to accomplish missions. Information superiority is not static; during operations, all sides attempt to secure its advantages and deny them to the enemy. The operational advantages of information superiority take several forms, ranging from the ability to create a superior common operational picture and understand it in context, to the ability to shape the information environment with information operations. Commanders attain information superiority by effectively integrating and synchronizing the three contributors—intelligence, surveillance, and reconnaissance (ISR); IM; and information operations (IO)—to enable and complement the full spectrum of military operations, portrayed in figure I-1.

c. Information superiority leads to decision superiority when the joint force commander makes better and faster decisions than those made by an adversary, or when his decision cycle becomes fast enough to anticipate and respond to changes in the operational environment. As one of three contributors to attaining information superiority, IM is a key integrator. Information is a critical component of combat power. Information

users at all levels need to change the way they think about information. The intent is to treat information as an asset, just like any other weapon or tool of warfare.

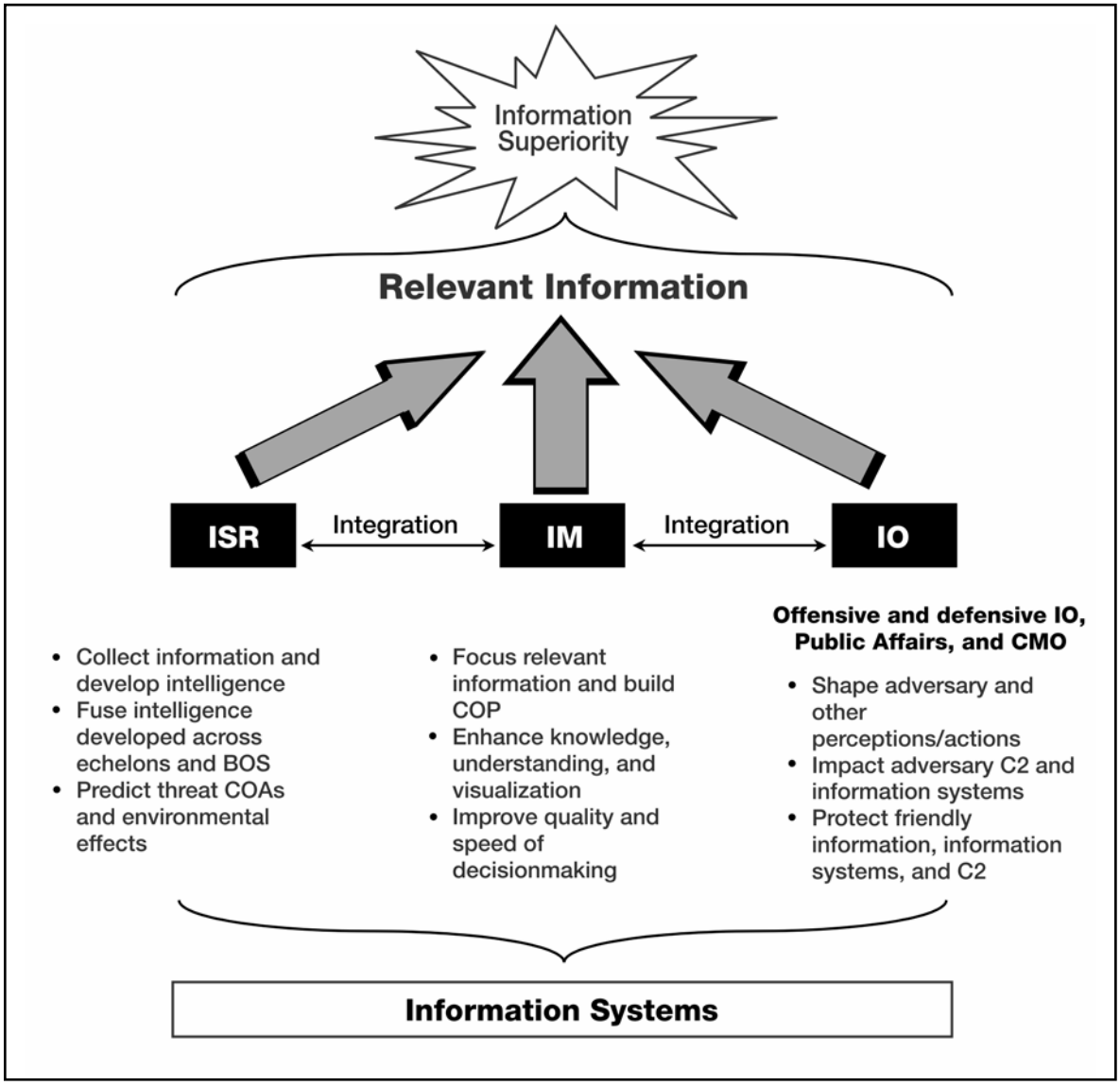


Figure I-1. Information Superiority—IM Relationship

3. Information Management

a. IM is the provision of quality information to the right person at the right time in a usable form to facilitate understanding and decisionmaking. The goal of IM is providing relevant, precise, accurate, timely, usable, and complete information that supports the commander in obtaining situational awareness and understanding that allows him to make timely and effective decisions faster than the adversary. It uses procedures and information systems to collect, process, store, protect, display, disseminate, and dispose of information.

Note: The Army uses the words "relevant information" instead of "quality information" in their definition of IM. The Army definition does not include "protect" and "dispose" as these are considered inherent to IM processing (FM 3-0).

b. IM is defined here within the context of decisionmaking and differs from the formal definition found in DOD Directive 8000.1. It defines IM as the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

4. Information Management Process and Activities

Personnel, equipment, communications, facilities, and procedures are essential to the commander to exercise command and control (C2). C2 supports the commander in three main areas: achieving situational awareness/understanding, making decisions, and communicating execution information to implement those decisions. Effective IM is critical to all three areas. IM is cyclical in nature and has four basic steps, which are depicted in figure I-2.

Note: The Army uses the term "situational understanding" instead of "situational awareness" to convey the thought that understanding, not awareness, is the basis for (and enables) correct decisions (FM 3-0).

a. Processes.

(1) Identify information requirements. IM begins with the identification and/or updating of information requirements. Information requirements are the criteria that must be known about the battlespace to enable mission accomplishment. Information requirements applicable to staff functions are referred to as information requirements (IR) while those that support the commander's decisions during the execution of battle command are referred to as commander's critical information requirements (CCIR). The IR and CCIR focus information collection and the processing of large quantities of information available so they can be distilled into relevant information.

(2) Collect and process information. The process continues with the collecting and processing of information to fulfill information requirements. Staff sections collect information to satisfy the requirements associated with their IR, while CCIR are disseminated to elements that can develop information applicable to the unit mission. The IM activities that comprise this step are discussed in greater detail in paragraph 4b.

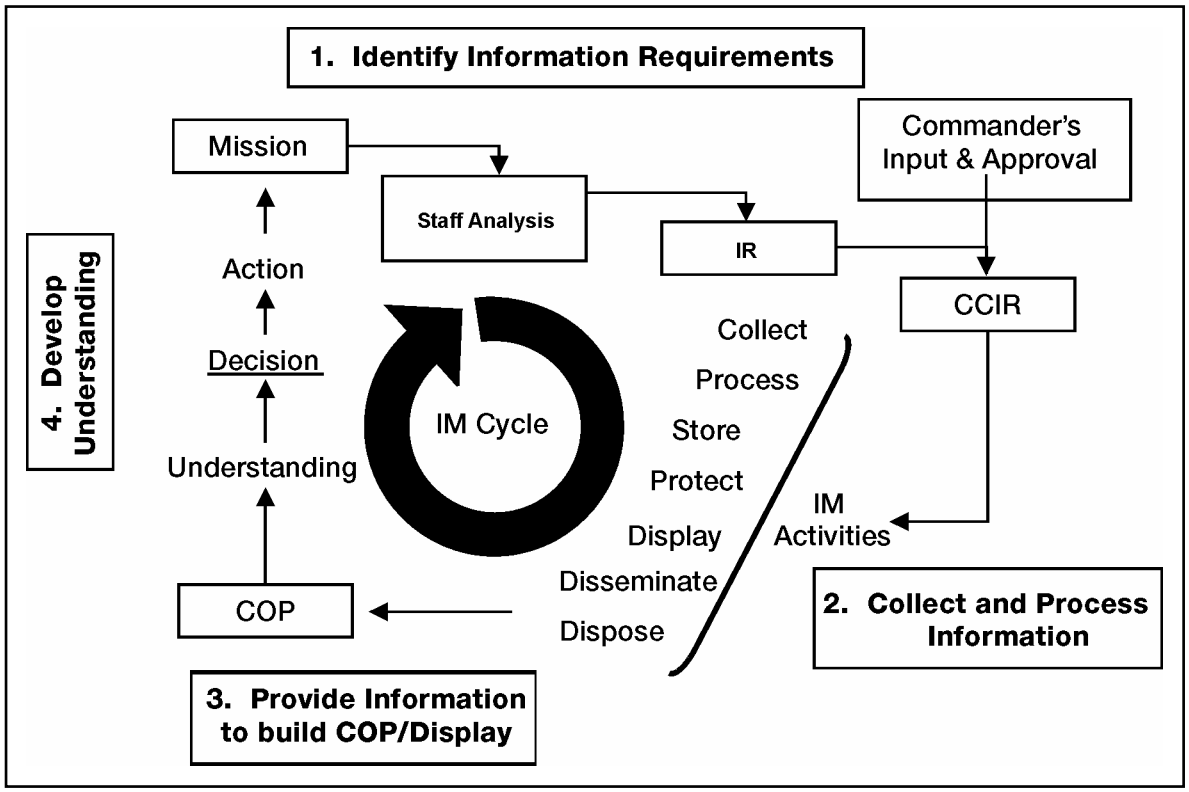


Figure I-2. Information Management Cycle

(3) Build a common operational picture (COP)/display. Information that is accurate, timely, usable, complete, precise, and reliable, is used to build a COP. As defined in JP 1-02, a COP is a single identical display of relevant information shared by more than one command. A COP facilitates collaborative planning and assists all echelons to achieve situational awareness. While the COP is intended to support the unit mission, staff elements may develop information displays specifically designed to support their operations. The key consideration for information displays is that they are organized and easily understood to enable rapid decisions.

Note: The Army defines COP as an operational picture tailored to the user's requirements, based on common data and information shared by more than one command (FM 3-0).

(4) Develop understanding. Awareness is provided by information but understanding is the result of judgment applied to that information. Understanding equals the knowledge of what is happening and why. It allows the anticipation of consequences of friendly and enemy actions and enables the correct decisions to be made. Thorough situational awareness and understanding is usually the result of collaboration and leads to decisions. With decisions made, subordinates are directed to take actions with their forces. Executing these actions results in the need to adjust information requirements based on the situation.

b. Activities. IM includes seven basic activities: collecting, processing, storing, protecting, displaying, disseminating, and disposing of information. These activities occur continuously throughout all phases of all operations and enable understanding and decisionmaking.

(1) Collecting – obtaining information in any manner, including sensing, direct observation, liaison with official agencies, or solicitation from official, unofficial, or public sources from the information environment.

(2) Processing – raising the meaning of information from data to knowledge. Processing consists of filtering, fusing, formatting, compiling, cataloging, organizing, collating, correlating, plotting, translating, categorizing, arranging, analyzing and/or evaluating. It also refers to the application of judgment to generate understanding. The primary purpose of processing is to add meaning to the identified and isolated information.

(3) Storing – the retention of information in any form for orderly, timely retrieval, and documentation until needed. In the world of the digital battlefield, storage often equates to database management. Common access databases provide resources for supporting widely disparate and distributed information needs and building effective COPs. They provide bridges allowing different systems with different purposes to share information and interoperate effectively. Multiple applications will use the same data simultaneously for different purposes to support multiple decisions across the battlespace.

(4) Protecting – measures taken to ensure the availability, integrity, authentication, confidentiality, and nonrepudiation of information and information systems. These methods protect critical information systems from corruption, intrusion, and destruction, while safeguarding the commander's mission.

(5) Displaying – representing information in a usable, easily understood audio or visual form tailored to the needs of the user. The display conveys the COP for decisionmaking and exercising C2 functions. Historically, the display of information has taken the form of formatted charts, written reports, verbal narrative reports, and graphic map displays. Information display technology includes interactive imagery continuously updated in real or near real time and accessible from remote locations. To convey information effectively, displays must—

(a) Use symbols, graphics, and terminology consistent with joint standards.

(b) Be clear, understandable, and intuitive.

(c) Consist of accurate, reliable, timely, and relevant information.

(d) Change promptly and easily with updates.

(e) Be interoperable among Service components and outside agency elements.

(6) Disseminating – communication of information from one person, place, or thing to another in a useable form by any means to improve understanding or to initiate or govern action. Effective dissemination requires detailed planning and coordination to ensure efficient transfer of information and must be incorporated into unit standard operating procedures (SOP).

(7) Disposing – actions taken on inactive records. These include destruction and archiving of information. It may include a transfer to a staging area or records center or a transfer from one organization to another.

5. Information Quality Characteristics

a. The JTF requires a continuous flow of quality information to support operations. The goal of IM is to ensure that this quality information gets to the right place on time and in a form that is quickly useable by its intended recipients. Quality information must meet the criteria listed below in figure I-3.

ACCURACY Information that conveys the true situation
RELEVANCE Information that applies to the mission, task, or situation at hand
TIMELINESS Information that is available in time to make decisions
USABILITY Information that is in common, easily understood format and displays
COMPLETENESS Necessary information required by the decision maker
BREVITY Information that has only the level of detail required
SECURITY Information that has been afforded adequate protection where required

Figure I-3. Information Quality Criteria

b. Information that is incomplete or imprecise is no better than no information; information that is untimely or not in a usable form is the same as no information; and information that is inaccurate or irrelevant is worse than no information at all. In general, a commander does not require information beyond a moderate level to accomplish the mission, as long as it is relevant, accurate, timely, and usable. Beyond that, a commander can achieve mission success at reduced cost when he has more information. However, collecting more information may carry an unacceptable cost in timeliness.

6. Cognitive Hierarchy

The IM process focuses on reducing uncertainty and increasing the commander, joint task force's (CJTF) situational awareness, supporting his decisionmaking, and preparing and communicating execution information for subordinates' action. IM processes use data and information that have been processed or displayed in a form that is understandable to the personnel using them and enhances situational awareness. We use the term information generically to refer to everything from data on the one hand to knowledge and understanding on the other. It is important to recognize the four classes in the cognitive hierarchy (see figure I-4).

a. Data – raw signals or sensings detected by a sensor or collector of any kind (human, mechanical, or electronic) from the environment or communicated between any kind of nodes in any system or processed in any way. The facts and individual data are the building blocks of information.

b. Information – meaning that humans assign to data. This meaning results from procedures such as filtering, fusing, formatting, organizing, collating, correlating, plotting, translating, categorizing, and/or arranging data.

c. Knowledge – result of analyzing information and evaluating its meaning by placing information in context and applying cognition. The user begins to build an accurate picture of the situation through integrating and interpreting various pieces of processed data. At this level, the user begins to get a product that can be useful for understanding.

d. Understanding – knowledge that has been synthesized and had judgment applied to it in a specific situation to comprehend the situation's inner relationships. It is the highest level of information. The user gains understanding with synthesis and the application of judgment (a uniquely human characteristic) to knowledge of a specific situation. Situational understanding allows the CJTF to anticipate future events and be better prepared to make sound and timely decisions. The whole point of the cognitive hierarchy and IM is to support decision superiority by adding meaning to information as it is managed.

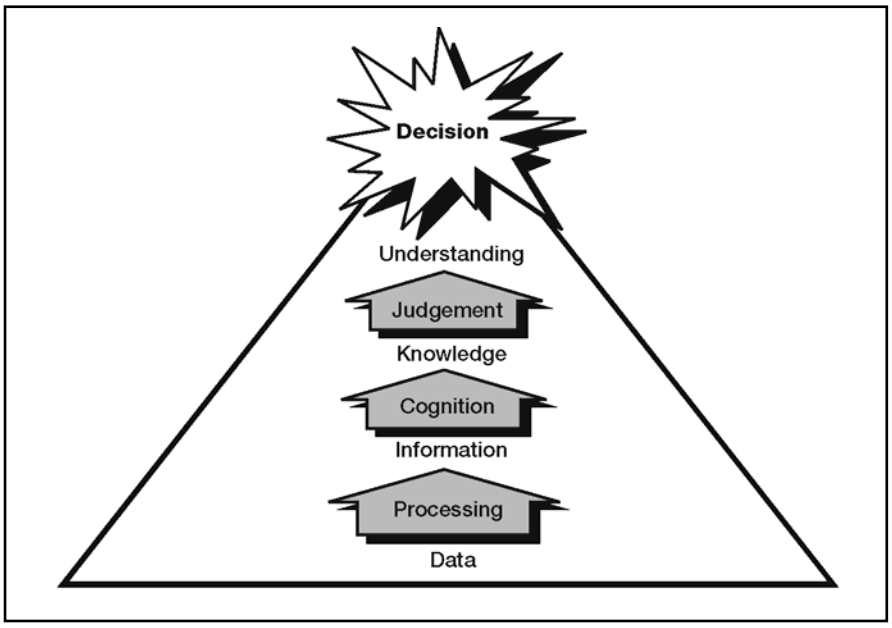


Figure I-4. Cognitive Hierarchy

7. Information Flow Strategy

JTF headquarters (HQ) IM procedures must provide for the rapid vertical and horizontal flow of information. Most JTF HQ staff processes require a cross-functional and cross-directorate exchange of information. Traditional staff arrangements help determine where information should flow within the organization, but should not form firewalls to the information exchange. Information flow within the JTF is a complex yet vital function for reducing uncertainty and ambiguity, while facilitating a clear understanding of the battlespace for the commander. While information and information products (such as intelligence) that represent knowledge can be disseminated, knowledge and understanding cannot be disseminated. Understanding relies more on the human quality of judgment and is therefore more difficult to share than knowledge, because knowledge products rely more on scientific processes, even when conducted by humans. Information flow strategy must account for this distinction.

a. Optimum information flow within the JTF requires both speed and clarity of transfer without creating fragmented or useless information. The IM plan (IMP) should assign responsibilities and provide instructions on managing information for the JTF. This a vital step, ensuring decisionmakers have the required information when they need it, and in an understandable format. Effective flow of information requires the information to be—

(1) Positioned properly. The JTFs needs for specific types of information are often predictable. Positioning the required information at its anticipated points of need speeds the flow and reduces demands on communications systems (for example, using public folders to post required information).

(2) Mobile. The reliable and secure flow of information must be commensurate with the JTFs mobility and tempo of operations. Information flow must immediately adjust to support the vertical and lateral flow of information between adjacent forces (for example, collaborative [integrated] planning system).

(3) Accessible. All levels of command must be able to pull the information they need to support concurrent or parallel planning and mission execution. If possible, channel information to the required user via automated means, reducing the need for manual exchange (for example, graphic depiction of forces in a COP).

(4) Fused. Information is received from many sources, in many mediums, and in different formats. Fusion is the logical blending of information from multiple sources into an accurate, concise, and complete summary. An objective of IM is to reduce information to its minimum essential elements and in a format that can be easily understood and acted on (for example, threat assessment disseminated in graphic form on an automated COP system).

b. The JTFs command, control, communications, computer, and intelligence (C4I) systems provide the means for information dissemination. Users of information are ultimately responsible for its management. Principal, special, and supporting staff directors or chiefs must clearly identify their information requirements and work closely with the JTF information management officer (IMO), ensuring processes are automated in the most effective way possible.

c. The IMP should include procedures to filter, fuse, and prioritize required information. This publication discusses these concepts.

(1) Filtering is a process of extracting information based on specified criteria.

(2) Fusion assesses information from multiple sources and develops a concise and complete summary.

(3) Prioritization focuses the efforts of the JTF HQ on developing information supporting the JTF commander's decisionmaking process.

8. Information Management Plan

a. To reach the goal of information superiority, the JTF needs to establish an effective IM organizational structure and IM flow strategy to track, control, and fuse the vast amounts of information used by the JTF. The information flow strategy is designed to meet the commander' s needs for relevant and timely information, while optimizing the use of information infrastructure resources. The JTF IMP should assign responsibilities and provide instructions on managing information for the JTF. This vital step ensures

decisionmakers have the required information when they need it and in an understandable format.

b. IM requirements vary, and this publication cannot cover all of the possibilities. Therefore, a JTF must develop an IMP tailored to manage information within the context of its mission and capabilities. An effective IMP provides guidance ensuring the availability of "quality information" throughout the JTF HQ. The CJTF can then correctly assess changing conditions, establish priorities, and facilitate the decisionmaking process. An IMP checklist is located at appendix C. Appendix C also has links to examples of IMPs currently in use.

Chapter II
IM ORGANIZATION, DUTIES, AND RESPONSIBILITIES

1. Introduction

This chapter identifies organizational structure, principal managers, and their key duties and responsibilities. An organized and disciplined effort by all personnel is necessary to ensure the right information gets to the right person at the right place and time in the right format to facilitate situational awareness and decisionmaking in a joint force environment. A further responsibility is to protect this information from unauthorized use or dissemination.

a. Most often, joint forces are organized with a combination of Service and functional components, commands, and subordinate task forces with operational responsibilities. All joint forces include Service component commands, and may include functional commands depending on the specific mission of the joint force commander. Both Service and functional component commanders have the responsibility to treat information as an asset, just like any other weapon or tool of warfare.

b. A joint force commander may organize the JTF HQ as necessary to carry out all duties and responsibilities. There are several options that may be used to form a JTF HQ. When fully formed, the JTF staff will be composed of appropriate members in key positions of responsibility from each Service or functional component having significant forces assigned to the command. The CJTF will make the final decision on the composition of the JTF HQ, to include the establishment of information management boards, centers, and cells. JTF structure and their associated staff structures are described in more detail in JP 5-00.2.

c. To aid the commander in tracking, controlling, and fusing the vast amounts of information that a JTF can encounter, he will need to establish an effective IM organizational structure. For a large JTF, a group of individuals will be required to accomplish effective IM. No matter what the size, an IM organization will provide the JTF with an information flow strategy designed to meet the commander's needs for relevant and timely information while optimizing the use of information infrastructure resources.

d. Depending on its size, a JTF may use some, all, or none of the elements listed below to create an IM organization. Naturally, any JTF will have some form of an IMO. Figure II-1 shows a notional IM organization within a JTF. In this example, the IMO is reporting directly to the COS. An advantage of putting the IMO under the COS is to provide leverage to manage information management policies effectively within a JTF. In combat situations, however, the J3 may be best positioned to manage the IMO. Ultimately, the CJTF decides where to place the IMO function so he can best manage IM for the JTF.

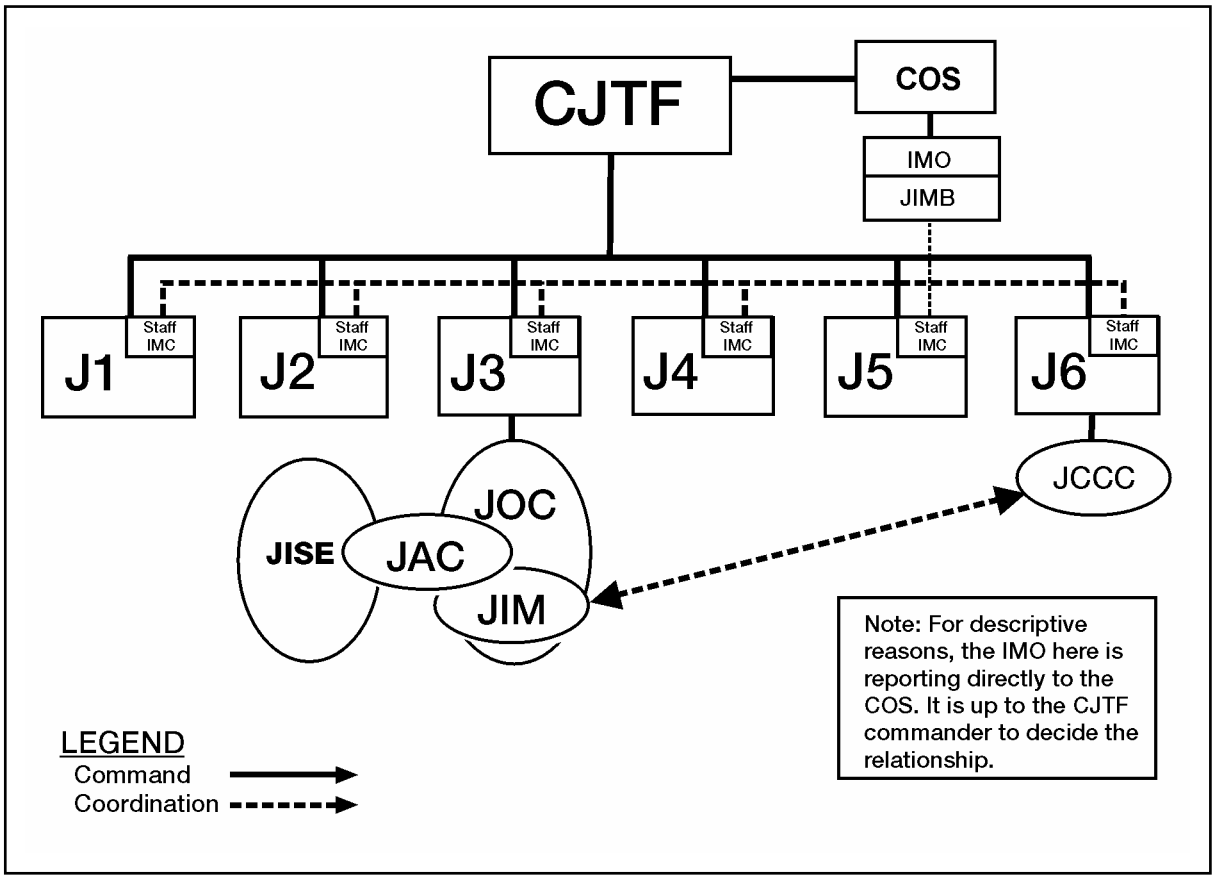


Figure II-1. Example of a JTF IM Structure

2. JTF Headquarters Responsibilities

a. CJTF. The CJTF—

(1) Approves the JTF IMP.

(2) Establishes priorities for information gathering and reporting by establishing the CCIR and commander's dissemination policy (CDP) as outlined in chapter III.

(3) Approves the JTF communications and information annex to the operations order/plan.

b. JTF COS. The JTF COS—

(1) Approves the JTF HQ daily operations cycle/battle rhythm, outlined in chapter III.

(2) Establishes a joint information management board (JIMB).

(3) Implements and enforces the JTF HQ IMP.

(4) Appoints the JTF IMO.

(5) Appoints the JTF RFI manager.

(6) Determines liaison requirements, establishes liaison information exchange requirements, and receives liaison teams.

c. Principal JTF staff sections. The principal JTF staff sections—

(1) Implement internal staff section procedures to comply with the IMP.

(2) Appoint a staff section information coordinator (IMC).

(3) Appoint a web content manager for their section. (This may be combined with the information manager in a smaller staff.)

(4) Are responsible for training and enforcing compliance with basic IM and security procedures for all staff section personnel.

(5) Provide information as required to support the IMP.

(6) Appoint a records custodian for their section.

(7) Appoint a workgroup manager for their section.

Note: This is an Air Force requirement that may have value to JTF staffs, as the workgroup managers are the first level of systems support and are an extension of the J6 help desk.

---

d. J2 and J3 appoint a request for information (RFI)/request for assistance (RFA) manager to accomplish RFI responsibilities.

e. JTF command, control, communications, and computer systems directorate (J6). The J6—

(1) In consultation with the JTF IMO and JTF staff elements, develops the JTF communications plan (annex K) to include the establishment of C2 systems architecture.

(2) Establishes a joint communications control center (JCCC).

(3) Establishes a technical help desk for network and systems administration issues for information systems (for example, collaboration software and Global Command and Control System [GCCS]).

(4) Assists the IMO in the development of digital rules of protocol (DROP).

(5) Processes security accreditation packages for CJTF approval.

(6) Establishes network and E-mail accounts, JTF telephone directories, and E-mail global address lists, as outlined in chapter III.

(7) In consultation with the IMO and JIMB, consolidates and validates a list of communication and system requirements based on validated IERs. Ensures compliance with the joint technical architecture and submits validated list to the COS.

(8) Oversees process of providing network status and network architecture to the JOC, via the JCCC.

(9) Establishes information assurance (IA) procedures in accordance with the IMP.

(a) Coordinates IA policy and strategy development throughout the entire JTF.

(b) Ensures IA is integrated into deliberate and crisis planning processes.

(c) Promulgates policy for inclusion to the IMP.

(d) Coordinates with the JCCC and JIMB for configuration policy management.

(e) Liaisons with the joint information management (JIM) cell or designated JOC IO cell representative.

(10) Plans for, and ensures, network and communications/computer system training and familiarization for JTF staff and augmentees is accomplished.

(11) Plans and ensures that deployed non-military information systems are open and nonproprietary, with commonly accepted standards and protocols that interoperate with military information systems.

(12) Manages network drive storage, and backs up and restores network drive data.

(13) Appoints the JTF web administrator.

(14) Appoints the JTF records manager.

f. JOC. A JTF will often organize a JOC to serve as a focal point of all operational matters. The JOC manages friendly and enemy information by maintaining situational awareness. It also maintains the status-of-forces and promulgates CJTF orders in the execution of current operations. The JOC—

(1) Tracks and fulfills all approved CCIR, unless a JOC/JISE assessment cell (JAC) is formed.

Note: The term JAC is defined in JP 1-02 as joint analysis center. For brevity reasons, JAC will be used solely in this publication as the JOC/JISE assessment cell.

(2) Recommends the addition of new, or archiving of existing, CCIR to the J3, unless a JAC is formed.

(3) Assesses the information flow to support JTF operations and monitors the efficiency, effectiveness, and accuracy of the JTFs COP.

(4) Maintains a master suspense action log.

(5) Maintains a chronological record of JTF significant events.

(6) Is responsible for the CJTF's daily briefings and fragmentary order (FRAGO) production.

(7) Works closely with the JISE to assess, update, and integrate information requirements.

(8) Reviews and records incoming message traffic.

(9) Creates and submits a battle rhythm for COS approval.

3. Joint Information Management Cell

Depending on the size of the JTF and scope of operations, the JTF COS may establish a JIM cell within the JOC. The JIM cell reports to the JOC chief (or possibly the J3), and facilitates information flow throughout the JTF area of operations. In absence of a

standing JIM cell, the responsibilities defined below must be assumed by other positions within the IM structure.

Note: The earlier version of this document referred to a common operational picture cell or board (COPC/COPB). All COPC/COPB functions have been incorporated into the JIM cell, however commanders may build such IM organizations based on the situation. Additionally, the IM cell or function may be referred to by other names depending on the command or unit. The JIM cell—

a. Is responsible for ensuring the CDP is implemented as intended by the CJTF.

b. Takes guidance published in the CDP and combines it with late-breaking operational and intelligence information obtained from the JOC/JAC.

c. Works closely with the JCCC to coordinate potential changes in communications infrastructure to meet late-breaking changes in the commander's information dissemination requirements.

d. Coordinates the accurate posting of all current, approved CCIR.

e. Acts as the focal point for coordinating the COP within the JTF.

f. Reviews and validates subordinate data inputs to provide an accurate COP for the JTF.

g. Is actively involved in resolving all cross-functional COP issues.

h. Advocates to the components to establish their own COP point of contact (POC) to manage the component's portion of the JTF's picture.

4. Joint Intelligence Support Element

The JISE, if formed, is the hub of intelligence activity in the joint operations area (JOA). A technique to ensure efficient IM is to co-locate JISE current situation analysts with the current operations analysts. This technique reduces any need for additional manpower. The JISE—

a. Maintains operational awareness of the battlespace by fusing and assessing all friendly and enemy information, unless a JOC/JISE assessment cell (JAC) is formed.

b. Reviews the enemy and friendly situations to conduct a complete and thorough assessment, unless a JOC/JISE assessment cell (JAC) is formed.

c. Is responsible for providing the JTF commander, staff, and components, with the complete air, space, ground, and maritime adversary situation.

d. Integrates and adds to the adversary situations developed by the combatant commander's intelligence organization.

5. JOC/JISE Assessment Cell

During operations, massive amounts of data flow into the JOC and the JISE from myriad sources. The personnel assigned to the JOC/JISE must filter, sort, and process data into information. That information must be fused, analyzed, and converted into knowledge. An additional option to integrate friendly/enemy intelligence and operations information is

to establish an information fusion cell known as a JOC/JISE assessment cell (JAC), which reports to both the J3 and J2. This option may be most effective in large, long-standing JTFs where the volume of information flowing into the JOC may become so large as to become lost. The JAC provides assessments of the current situation with recommendations to the J3. The JAC—

a. Tracks and fulfills all approved CCIR.

b. Recommends the addition of new, or archiving of existing CCIR to the J3.

c. Maintains operational awareness of the battle space by fusing and assessing all friendly and enemy information.

d. Reviews the enemy and friendly situations to conduct a complete and thorough assessment.

6. Joint Information Management Board

The JIMB is responsible for building the CJTF's IMP. The JIMB is the action arm of the JTF IMO and is comprised of membership from all functional areas within a commander's staff. The JIMB is co-chaired by the J6 and draws on the expertise of each functional area within the CJTF's staff. The JIMB—

a. Builds the IMP.

b. Identifies and validates IERs and provides them to the J6.

c. Acts as the focal point for coordinating IM policy within the JTF.

d. Operates under the supervision of the COS, or appropriate staff directorate, as best meets the JTFs mission needs.

e. Resolves cross-functional and contentious information management issues.

7. Information Management Officer

The IMO leads the JIMB. The IMO is the senior information manager within the JTF. The IMO coordinates information flow within and to/from the JTF and establishes policies and systems to enable efficient and effective processes are compatible and integrated into the JTF IM structure as a whole. The IMO—

a. Ensures the JTF IM system accurately reflects the JTF IMP.

b. Approves format and structure of information posted and distributed from the JTF (briefings, reports), using the JIMB.

c. Develops and publishes the JTF HQ IMP, to include digital rules of protocol (DROP).

d. Coordinates additional training requirements by staff and component elements to support IM.

e. Works closely with the JIM cell to develop effective and efficient JTF COP management procedures.

8. Staff Section Information Management Coordinator

The staff IM coordinator (IMC) represents each functional directorate at the JIMB. The staff IMC is the functional director's advocate for all IM related matters. The staff section IMC—

a. Oversees the internal and external information flow of their staff section.

b. Provides the JTF IMO with staff section information exchange requirements for incorporation into the JTF IMP.

c. Provides the JTF J6 a list of their requirements for network support.

d. Ensures compliance with the JTF IMP.

e. Coordinates and conducts internal IM training for staff section members.

9. JTF Components and Supporting Agencies

Each component and supporting agency should—

a. Appoint an IMO as a primary point of contact for IM matters to implement JTF IMO functions at the component level.

b. Appoint a web content manager as a primary point of contact for web administration.

10. JTF Website Administration Responsibilities

The JTF must identify three distinct roles to support network centric operations and establish their responsibilities: JTF web administrator, staff web content manager, and information producer.

a. JTF web administrator. The web administrator is responsible for the overall management of information on the JTF web site. The web administrator must coordinate with the various staff sections, components, and supporting agencies ensuring establishment of the web site infrastructure facilitating the necessary information exchange throughout the JTF. The web administrator is a technical role and requires an understanding of employed web technologies. The web administrator ensures maintenance of the posted information in accordance with the IMP and the CDP.

b. Staff web content manager. The staff web content manager ensures website information within their directorate is kept current and meets the requirements of the IMP and CDP. He coordinates technical change requirements with the JTF web administrator.

c. Information producer. Each component, supporting agency, and JTF staff section, as producers of information, determines what information they create and maintain on the JTF web site. The information producers are responsible for keeping their staff web content manager informed on changes to ensure sites are current and accurate in accordance with web policy and the IMP.

11. Records Management

The JTF must identify four distinct records management roles to support network centric operations and establish their responsibilities for ensuring the operational availability of records: records manager, records custodian, action officers, and the JCCC.

a. Records manager. The records manager is responsible for the overall management of records residing in the JTF, regardless of media. The records manager establishes and administers the JTF records management program. See appendix B, paragraph 2a and 2b, for a list of specific responsibilities.

b. Records custodian. The records custodian is responsible for the management of division or section records. See appendix B, paragraph 2c for a list of specific responsibilities.

c. Action officers. Action officers are responsible for working with their records custodians to properly control, protect, classify, and file all information for which they are responsible in accordance with appropriate records management policies. See appendix B, paragraph 2d, for a list of specific responsibilities.

d. JCCC. The JCCC is responsible for backing up and restoring network drive data. See appendix B, paragraph 2e, for a list of specific responsibilities and procedures.

12. JTF Information and Information System Protection Responsibilities

a. Information security manager. The information security manager is responsible for the proper accountability, control, personnel access, and physical security/storage of non-compartmented Department of Defense (DOD) classified data, in both hard and soft-copy forms. Each JTF staff directorate normally appoints a security manager. See DODD 5200.1-R and applicable Service regulations for additional details.

b. Special security officer (SSO). The SSO is responsible for sensitive compartmented information (SCI) management, controls, and access. This responsibility is normally a JTF J2 function.

c. Operations security (OPSEC) officer. The OPSEC officer is responsible for oversight and implementation of the JTF's OPSEC program. This position is normally a JTF J3 function.

d. Designated Approving Authority (DAA). The DAA ensures, implements, and monitors a reliable information security (INFOSEC) program. The function of the DAA for all JTF information systems, with the exception of those systems processing SCI, is normally a responsibility of the JTF J6. DAA for SCI information systems is handled via the SSO. The DAA has the following responsibilities:

(1) Accredits all automated information systems (AIS) under their jurisdiction before placing them into operation.

(2) Allocates resources (funding and manpower) to achieve and maintain an acceptable level of protection and to remedy security deficiencies.

(3) Makes sure certifying officials, functional offices of functional responsibility (OPRs), and information systems security officers (ISSO) are identified for all AIS under their jurisdiction.

(4) Approves system security policies.

e. Information systems security manager (ISSM). Normally a JTF J6 function, the ISSM is the focal point and principal advisor for INFOSEC matters on behalf of the DAA. The ISSM has the following responsibilities:

(1) Develops, implements, and maintains the JTF staff INFOSEC plan for all systems operated in the command.

(2) Ensures ISSO and other information system security staff are properly trained and appointed in writing.

(3) Assists ISSOs with preparing accreditation support documentation including risk assessment documentation, security test and evaluation (ST&E) documentation, and contingency plans.

(4) Ensures that configuration management of staff hardware and software complies with the INFOSEC plan.

f. ISSO. The ISSO is normally a JTF J6 responsibility. The ISSO is responsible for implementing and maintaining security on behalf of the ISSM. The ISSO reports to the JTF ISSM for INFOSEC matters and implements the overall INFOSEC program approved by the DAA. Each staff directorate in the JTF organization appoints an ISSO in writing. Larger directorates may appoint multiple ISSOs. Forward ISSO appointment letters to the ISSM. The ISSO is the point of contact for IS matters within his selected area of appointment, with the following responsibilities:

(1) Develops a system security policy for AIS and networks that process or protect sensitive unclassified and classified information.

(2) Makes sure that audit trails are reviewed periodically (for example daily, weekly, etc.).

(3) Performs an initial evaluation of each vulnerability or incident, begins corrective or protective measures, and reports according to established network incidents reporting procedures.

(4) Notifies the DAA when AIS are involved.

(5) Evaluates known vulnerabilities to ascertain if additional safeguards are needed.

(6) Coordinates with the ISSM on matters concerning INFOSEC.

(7) Ensures information system security procedures are implemented within their assigned area.

(8) Ensures users within assigned areas are operating, maintaining, and disposing of systems per INFOSEC policies and procedures.

(9) Trains the IM users within the assigned area on INFOSEC responsibilities.

(10) Ensures personnel and physical security requirements are followed.

g. Network security officer (NSO). The NSO is normally a JTF J6 function. The NSO is responsible for implementing and maintaining network security on behalf of the ISSM. The J6 appoints the NSO, who has the following responsibilities:

(1) Ensures incorporation of countermeasures and safeguards in the network design and daily performance of the network.

(2) Informs the ISSM of external network connection requirements so the ISSM can request memorandums of agreement (MOAs).

(3) Develops and promulgates the standard INFOSEC procedures governing network operations.

(4) Ensures security measures and procedures used at the network nodes fully support the security integrity of the network.

h. Terminal area security officers (TASO). When needed, the officer-in-charge for each remote site, with a terminal connection to a network, designates a TASO in writing. The TASO is the representative of the ISSM or ISSO in matters pertaining to the security of each terminal. Each JTF HQ staff directorate operating both a classified and unclassified network terminal normally appoints TASOs. The TASO enforces all applicable security requirements implemented by the INFOSEC program and the ISSM.

13. JTF Information and Information System User Responsibilities

Every user has inherent responsibilities to acquire, assess, reason, question, correlate, and disseminate quality information to other users.

a. The JTF information and information system user responsibilities are to—

(1) Ensure accuracy, relevance, timeliness, usability, completeness, brevity, and security of JTF information.

(2) Properly control, classify, protect, and archive all JTF information and information systems for which they are responsible in accordance with appropriate records, management policies (see DODD 5015.2, CJCSI 5760.01, CJCSM 5760.01 Volume 1 & 2, and appendix B for an example).

(3) Validate the authority to dispose of JTF information before destruction.

(4) Read and comply with the information requirements published in the JTF IMP.

b. As information users, each member of the JTF must continuously ask the following four questions:

(1) Does the information I need already exist? Time is wasted developing information (point papers, briefings, etc.) if the information already exists. Responding to multiple requests for the same information is wasted effort. One solution is developing a collaborative (integrated) planning system that supports information requirements necessary to support planning, decisionmaking, execution, and assessment.

(2) Who else needs the information? Sharing information is essential to maintain unity of effort and synchronization of operations. Users must consider who (higher, lower, and laterally) requires the information to assist in developing solutions.

(3) What is the most efficient and effective way to transfer the information? Many times the initial reaction to receipt of seemingly important information is sending an e-mail to “all JTF staff.” Web sites and public folders are increasingly popular for transferring important information. However, posting information to a homepage or public folder is no guarantee of receipt by the intended audience. Understanding the “process” (information flow) that satisfies each essential JTF requirement enables all personnel to determine the most efficient and effective means to transfer information. A few moments of consideration assists in determining what is the best, most timely, efficient, and effective method of notifying the appropriate JTF staff members. Consideration must be given to whether

using web sites, or public folders are timely for critical actions, such as transmitting FRAGOs or warning orders. Occasionally, direct contact is a more appropriate means.

(4) "How do I add meaning to this information?" Knowledge is more than just simply organizing information. Knowledge results when information is placed in a context that leads to understanding. CCIRs are an example of how information can be placed in a context chosen by a commander.

Chapter III
IM REQUIREMENTS, PROCESSES, AND PROCEDURES

1. Background

Using the IM organization, duties, and responsibilities described in chapter II, the CJTF can be provided the quality information needed to conduct operations. This chapter describes the requirements, processes, and procedures these organizations use to develop an information flow strategy that supports the CJTF in making informed decisions. The organization using the flow strategy will fuse the massive amounts of data flow from myriad sources into knowledge that can lead to superior decisionmaking

2. Processes

a. To accomplish the management of essential information and perform appropriate C2, the CJTF may establish a JOC. The JOC should be staffed and equipped to manage friendly and enemy information, maintain the tactical situation and status-of-forces, make recommendations, and promulgate CJTF orders in the execution of current operations.

b. Central to the success of meeting the operational needs of the user is the JTF IMO, the JIMB, the JAC, and the JIM cell. Chapter II describes these entities, their location within a JTF structure, and roles and responsibilities in more detail. Figure III-1 shows information flows of IM planning within a JTF. Figure III-2 shows the organizations, relationships, and IM operations information flow within a JTF.

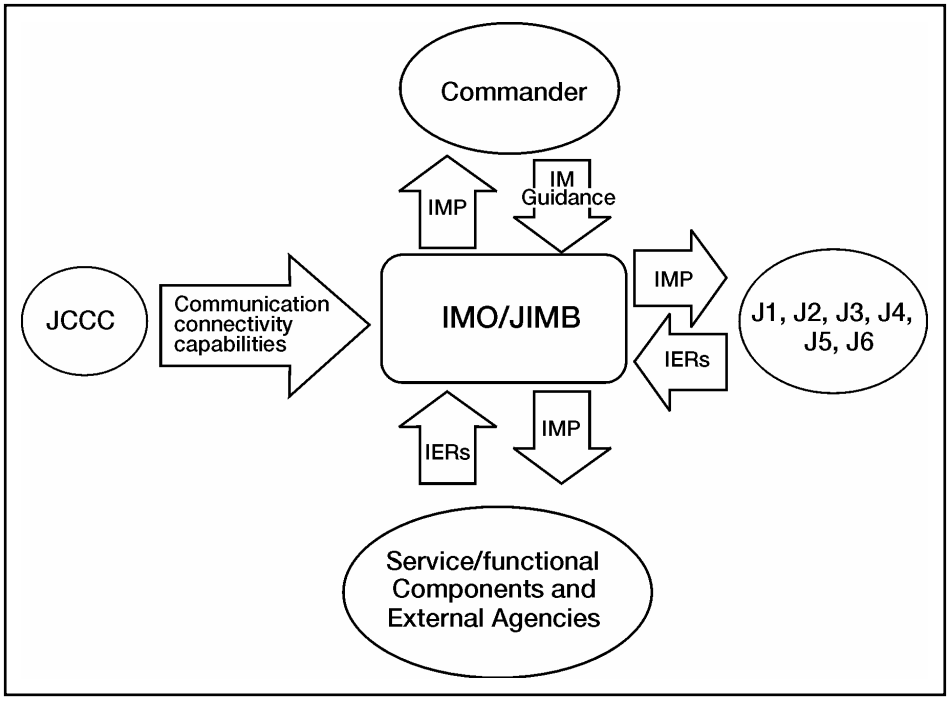


Figure III-1. JTF IM Planning Information Flow

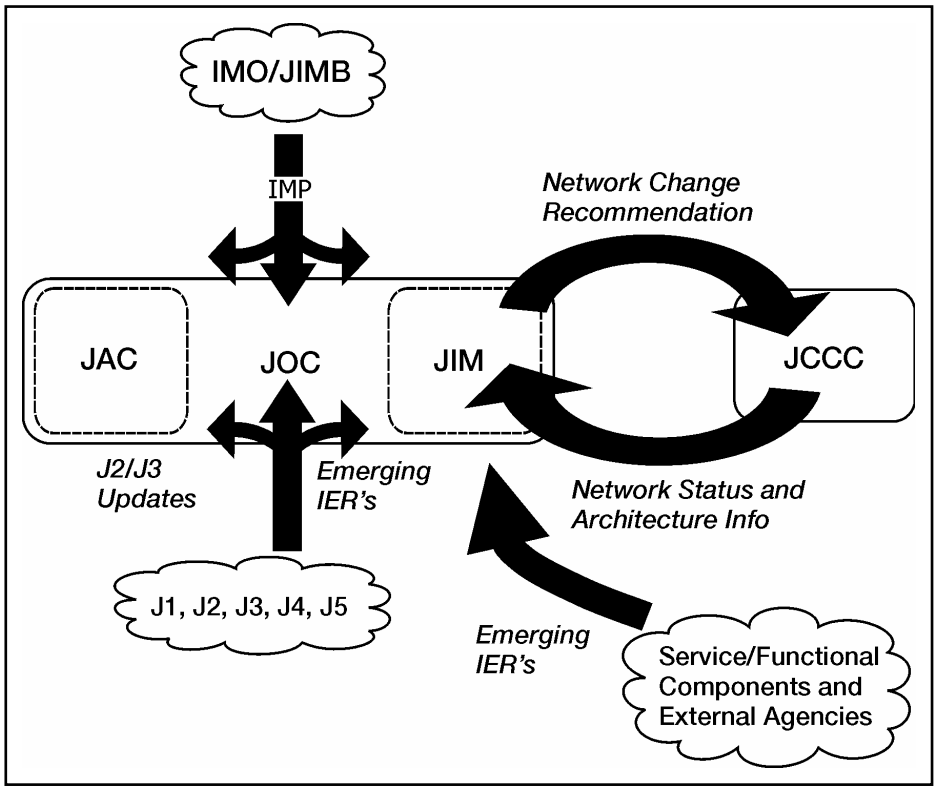


Figure III-2. JTF IM Operations Information Flow

(1) JTF IMO. The IMO leads the JIMB. The IMO is policy focused, is the senior information manager within a JTF, and is responsible for developing and publishing the commander's IMP. The IMP covers the commander's IM requirements and is described in more detail in this chapter, paragraph 4. The IMO coordinates IM issues closely with the JIM cell.

(2) JIMB. The JIMB is policy focused and responsible for building the JTF's IMP. As the action arm of the JTF IMO, the JIMB works closely with the staff section information managers to build the IMP. This board meets to build the IMP and periodically is required to make updates or changes. To accomplish its function, the JIMB should include:

(a) JTF IMO – leads JIMB.

(b) Staff section IM coordinators.

(c) COP manager.

(d) JCCC representative.

(e) JIM representative.

(f) RFI manager.

(g) IA representative.

(h) Web/database administrator/manager.

(i) External organization representatives, as required.

(j) Records manager.

(3) JAC. A technique for fusing information between the intelligence and operations is the use of a JAC cell.

(a) Role of the JAC Cell. As the fusion cell between the J2 and J3, the JAC provides analysis and assessments of operational and intelligence information in response to CCIRs and emerging operations/intelligence issues occurring in the battlespace. The JAC analyzes and fuses enemy/friendly intelligence and operational information and provides results of the assessment with recommendations to the J3. After review, the JAC recommends the addition of new or archiving of existing CCIRs to the J3 for accurate posting of all current, approved CCIR in the JOC.

(b) Reporting and coordination. The JAC reports to the J2 and J3. If the staff principles are not available, it reports to the deputy JOC chief. The JAC coordinates with the JISE chief as required. The JAC receives primary information from the current operations/current intelligence cells. This may mean the JAC is located within the joint intelligence center (JIC) or in other SCI-level spaces.

(c) Function. The JAC's function is to maintain operational/situational awareness and contribute to the understanding of the battle space by the constant fusion and assessment of all friendly and enemy information. The JAC has no tasking authority over the watchstanders in the JOC. It is incumbent on the J3 to ensure the JAC receives all required information to accomplish its mission. The JAC keeps the J3 informed. The JAC also assesses the friendly and enemy situation to build situational awareness, support achieving situational understanding, and enhance decisionmaking for the CJTF. Subsequently, the JOC and JISE must continuously report confirmed, accurate, filtered, processed and categorized information to the JAC. The JAC then analyzes and fuses this information for each appropriate specialty. After this analysis is complete, they present this information and recommendations to the J3 for possible action. The JAC answers the questions of "what is our situation...what is the enemy's situation...what does it mean to our current operations?" The JAC's mission is critical to the success of the JTF mission. Accordingly the J3 must ensure the JAC's role stays focused on its mission and is not tasked with additional duties.

(d) Organization. The list below is one recommended solution for staffing the JAC. Each JTF must evaluate its mission and then establish the manning level and required personnel specialties for the JAC. Each shift of the JAC should be comprised of individuals with specialties tailored to the JTF mission. JAC personnel must have Service experience, appropriate qualifications, and subject matter expertise. They should have a diverse background to grasp the concepts required to fuse and analyze information regarding joint operations. Joint warfighting or joint staff experience is a plus. The senior officer assigned in the JAC is designated the JAC chief. An example of a JAC may include the following skill specialties:

- Ground operations.
- Naval operations.
- Air operations.
- Intelligence.
- Special operations.

- IO.
- IM support.

(4) JIM Cell. A JIM cell may be established in the JOC to facilitate information flow throughout the JOA. The JIM cell, responsible for implementing the CDP, ensures the right information gets to the right person in the right format at the right place and time.

(a) Because the JIM cell is focused on information throughout the JOA, the JIM cell works closely with the JCCC to coordinate potential changes in communications infrastructure to meet changes in the commander's information dissemination requirements. The JIM cell's activities include management and manipulation of the COP.

(b) The JIM cell may include:

- JIM chief (officer with operational and information management background).
- Air, land, sea, and threat force track managers (for example, joint interface control officer [JICO]).
- COP manager.
- Information technology (IT) support personnel.
- JCCC liaison officers.

3. Information Management Plan

Each organization has unique information requirements directly affecting decisions and successful operations. The JTF JIMB must develop an information management plan tailored to manage information within the context of a JTF's missions and capabilities. An effective management plan provides guidance to ensure availability of decision-quality information. A plan is needed to articulate not just the processes that exist, but also the means by which the JTF will perform those processes. This plan is the JTF IMP.

a. The JTF IMP should cover all JTF IM needs. These include the duties, responsibilities, skill requirements; IM systems and requirements; IM processes and procedures; and IM system protection. The JTF IMP may include specific guidance for the management of the following. This MTTP is organized in a similar manner as an IMP and can be used as a template to follow when building an IMP. See appendix C (IMP Checklist) for a detailed breakout. Some of these items are:

(1) Commander's Dissemination Policy.

(2) Information requirements and general procedures (COP management, CCIR).

(3) Digital rules of protocol.

(4) Battle rhythm/schedule of events.

(5) IA/computer network defense (CND).

(6) Information systems (INFOSYS) tools and procedures (to include collaborative planning tools).

(7) Request for information (RFI) management procedures.

(8) Network applications and architecture. This guidance may include using records management, web pages, or other applications.

(9) Reports management.

(10) Master suspense action log (MSAL).

(11) Significant events log.

(12) Orders distribution.

(13) System recovery procedures.

b. CDP. The CDP serves as the commander's guidance portion of the IMP on dissemination of information within and outside of the JTF. The CDP is not a separate document, but a part of the IMP. It provides a foundation for developing the IMP and aids in prioritizing IM activities. It provides policy to guide JTF information management decisions in the absence of specific guidance or detailed instructions. Critical information needs must be predetermined and prioritized to ensure support for critical missions, prevent overload of routine information, and provide guidance to apportion information assets.

(1) The CDP (see figure III-3) may incorporate policies pertaining to:

(a) CCIR.

(b) Public affairs guidance.

(c) Communications network architecture.

(d) Release of real time operational information.

(e) Release of real time intelligence information.

(f) IO goals and objectives.

(g) Communications network status.

(2) Other areas a commander should consider for inclusion in the CDP are:

(a) Identifying the routine information products that must be sent to users based on their functional role(s) and/or mission(s).

(b) Weighting the main effort, allowing for dynamic adjustment to available bandwidth, and a reallocation of bandwidth to specific missions.

(c) Prioritizing information flow within an area of responsibility.

(d) Prioritizing requests for information based on:

- Specified user.
- Specified organization.
- Specified mission.
- Specified location.
- Information type (such as STRIKEWARNING, contact report).

(e) Overriding automatic assignment of priorities.

(f) Interfacing with databases and other information sources associated with building the COP and providing for rapid tailoring of information required to create a new or updated COP.

(g) Limiting access to specific information by content, source, type or location.

(h) Limiting file transfer sizes.

(i) Limiting information transfer due to security or classification policy and delivery tools.

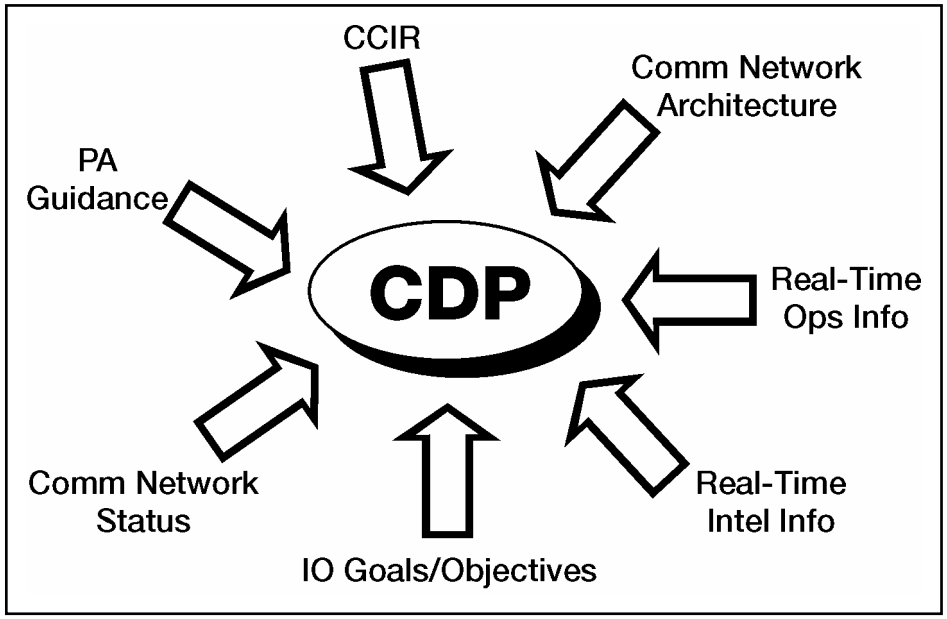


Figure III-3. Commander's Dissemination Plan (Notional)

4. Commander's Critical Information Requirements

a. CCIR are a comprehensive list of information requirements identified by the commander as being critical to facilitate timely information flow and the decisionmaking processes that affect successful mission accomplishment. For a more detailed description of CCIR, refer to the definition in JP 1-02 and the discussion in JP 3-0.

b. These information requirements, if met, provided, or reported, enhance the commander's ability to understand the flow of operations, identifying risk, and making timely decisions in order to set the conditions for success and retain the initiative. They reduce the data available to the commander to a manageable, finite set of information requirements, thereby avoiding information overload. CCIR focus the staff on the exact elements of information the commander must have as soon as it is available, and allow the staff to focus its efforts to acquire, process, filter, and fuse information in a time-sensitive manner. The key word is critical, and as such, the CCIR should not be voluminous. They should be dynamic, change by phase of the operation, and be tied to decision points. The JIMB needs to capture the process of developing, reviewing, and updating CCIR in the IMP.

c. Just as CCIR must be specific to focus information management and collection, CCIR is limited in number for any phase of an operation. Limiting the number of CCIR aids in comprehension and helps prioritize scarce collection resources. Additionally, CCIR is not static and may change as events unfold. Therefore, CCIR require continuous assessment for relevance to current and future situations. The following are some techniques for CCIR development and management.

(1) Review CCIR for each operation, branch, and sequel plan. During the planning process, staff directors may propose CCIR to the Joint Planning Group (JPG). The JPG chief consolidates the proposed CCIR for CJTF consideration and approval. After approval, the JOC posts the CCIR in an electronic medium (for example: CCIR, home page, etc.). An excellent example of this was the use of the CENTCOM Warfighter Web used in their forward headquarters in late 2002 and early 2003. This allowed CCIR to be posted in their portal and linked to the appropriate decision points. This causal link is extremely important and should not be overlooked.

(2) During the conduct of operations, review the CCIR continuously for relevancy. One technique is to review and modify the CCIR during the daily update briefing. Depending on the results of this review, CCIR elements may be modified or archived as necessary. The JTF staff should submit recommended changes to CCIR to the Director of Operations (J3). The J3 or JIMB reviews and compiles the recommended changes for presentation to the CJTF for approval.

d. All members of the JTF are responsible for reporting information that may satisfy CCIR. However, each staff director should ensure processes within their directorate are in place to filter and fuse raw data before submission. CCIR tracking/monitoring is a primary task of the JOC. When a CCIR is met, or there are indicators that one is about to be met, the JOC makes an immediate "voice" report to the CJTF, deputy commander, joint task force (DCJTF), principal staff directors, and component operations centers. Voice reports are followed by Flash messages via GCCS and E-mail to all staff directors and component commanders. When CCIR) are obtained, the JOC/JISE analyzes the implications on current and future plans, and then briefs the CJTF. This analysis should include any recommendations for modifications to or additional CCIR.

5. Requests for Information

a. The JTF HQ establishes RFI procedures to provide a systematic method for requestors to obtain information. More important than merely allowing requestors to get information is providing visibility to the rest of the organization on the questions and the answers to those questions. JP 1-02 defines requests for information as—"any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production". An RFI can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. RFIs are sent to higher, subordinate, adjacent HQ or to other agencies requesting the information necessary to support the planning and decisionmaking process (see figure III-4).

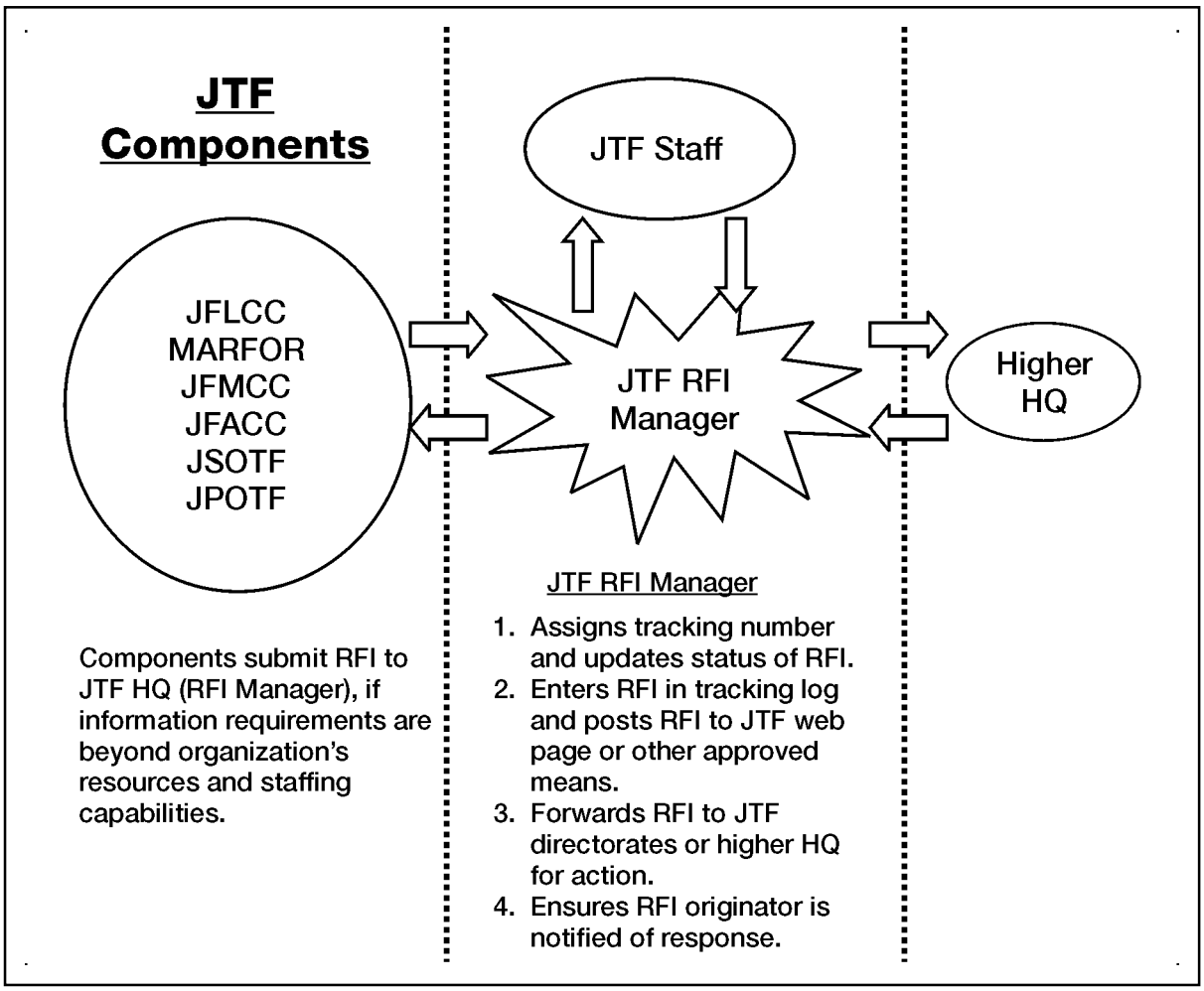


Figure III-4. Request for Information Flow Chart

b. The J2 processes intelligence-related RFIs, and the J3 all other RFIs. The J2 and J3 assign an RFI manager to receive and prioritize RFIs. A tracking system known as the community on-line intelligence system for end-users and managers (COLISEUM) is established to register, validate, track, and manage crisis and non-crisis intelligence information requirements. COLISEUM functions as an application on the joint deployable intelligence support system (JDISS) workstation, providing connectivity and interoperability with other intelligence systems supporting operational users. COLISEUM is supported on standard communication systems that are in compliance with validated joint architectures. For RFIs other than intelligence, table III-1 offers a sample method for RFI tracking.

c. Effective RFI procedures provide the JTF an "information pull" mechanism providing requestors access to a variety of vital information. RFI procedures do not replace normal staff coordination or substitute for researching information using other means (for example: intel link via the SIPRNET (and NIPRNET) available to JTF members. Instead, the RFI process provides a mechanism for a formal request to other echelons when the

issue or question is beyond the resources of the staff. The process also provides visibility of those requests forwarded, their status, and responses to these requests.

d. Components submit RFIs to the JTF HQs that are beyond their capability and staff resources to answer. Components submit intelligence related RFIs, in accordance with established procedures, to the JTF J2 RFI manager via COLISEUM, SIPRNET, e-mail, web pages, or other approved means. The JTF J2 RFI manager assigns an internal RFI tracking number only if not using COLISEUM for J2 RFI management. Components submit operational related RFIs to the JTF operations RFI manager (J3/J5), via SIPRNET E-mail/web pages or other approved means. The JTF operations RFI manager assigns an internal RFI tracking number, forwards it to the appropriate JTF staff directorate for action, then posts RFI responses to JTF web pages, or other approved means. If the JTF staff is unable to provide an answer, the JTF operations RFI manager forwards the RFI to higher headquarters for resolution.

e. Normally, RFIs are not necessary among JTF directorates. However, if a JTF is not in a single location or the RFI is exceptionally complex, the JTF staff section submits RFIs to the JTF RFI manager by posting it to a JTF web page or other approved means. The JTF RFI manager processes the request and forwards it to the appropriate agency for resolution. Each directorate is responsible for monitoring their RFIs and closing the request.

f. RFI Guidelines.

(1) Limit RFI to one question per request. (Multiple questions increase response time.)

(2) State RFI as a specific question and provide sufficient detail so the request is completely understood.

(3) Resubmit the RFI with additional comments or clarification, if a RFI is not completely answered.

(4) Submit a new RFI if additional information is required.

(5) Submit intelligence RFIs through the intelligence RFI system (COLISEUM).

(6) Spell out acronyms the first time they are used.

(7) Pass staff action RFIs to appropriate staff section.

(8) Include the following information in RFI request:

(a) Classification.

(b) Priority (Routine, Priority, Immediate, or Flash).

(c) Time/Date.

(d) Required not later than (NLT).

(e) Requestor.

(f) To (who should answer).

(g) Subject.

(h) Amplifying data (question).

(i) Recommended method of transmission.

(9) Intelligence related RFI requests include—

(a) Narrative description.

(b) Justification.

(c) Sources consulted.

(d) Date desired.

(e) Latest time information of value.

(f) Classification of response (desired class and accepted class).

(g) Remarks (any additional information not included in the narrative).

(h) POCs (include both the JTF RFI manager as well as the requester).

g. The RFI tracking log (table III-1) is a simple tool for use in a web page or other electronic medium. The purpose of this log is to provide JTF-wide visibility of the submitted RFIs and the status of responses. The status column of the request log is color-coded as follows:

(1) Red indicates a pending request.

(2) Amber indicates a response awaiting requester's review. The requester of an RFI closes all "amber" coded RFIs if the response answers the RFI completely by changing the status indicator to green.

(3) Green indicates that the RFI has been answered and that action is complete.

Table III-1. RFI Tracking Log

TRACK #	*TIME/DATE SUBMITTED*	*PRIORITY*	*REQUIRED NLT*	*SUBJECT*	*REQUESTOR*	*STATUS*
1						
2						
3						

6. Common Operating Picture Management

a. A JTF COP requires effective and efficient management procedures. Some of the data feeds into the COP are automatic and some are manual. Effective management of the COP prevents the display of outdated or unwanted information. The JIMB or JIM cell establishes procedures for updating and displaying relevant information.

b. The JTF COP manager (COPM) coordinates the actions required to synchronize and manage the COP information flow between the JTF components and the JTF HQ. The COPM should ensure the procedures identified in CJCSM 6120.01B are followed for track/location management on tactical data links between Service/functional components and subordinate echelons. The COP may require the following inputs:

(1) Blue/friendly air, maritime, and ground force tracks/locations within JOA.

(2) Red/enemy air, maritime and ground force tracks/locations within the JOA.

(3) White/neutral/unknown air, maritime and ground force tracks/locations within the JOA.

(4) Operational overlays.

(5) Intelligence overlays.

(6) National Imagery and Mapping Agency (NIMA) products.

(7) Fire support coordination graphics.

(8) Any other information or graphic displays required by the CJTF.

7. Joint Task Force Daily Operations Cycle (Battle Rhythm)

JTF information requirements are often predictable. The JTF HQ staff can position information at its anticipated points of need to speed information flow and reduce demands on communications systems. One method is establishing a daily operations cycle for briefings, meetings, and report requirements, etc. Table III-2 depicts an example.

Table III-2. Sample JTF HQ Daily Operations Cycle

LOCAL	*ZULU*	*EVENT*	*PARTICIPANTS*	*LOCATION*
0900	1400	Shift Change CJTF VTC with Components		
1000	1500	JFACC VTC		
1100	1600	JOC/JISE Update		
1200	1700	Plans Synchronization Meeting		
1300	1800	J2 VTC with Components Press Conference		
1400	1900	Future Plans Update to CJTF		
1500	2000	J3 Staff Meeting		
1600	2100	JPG Plans Synchronization Meeting		
1700	2200	Component SITREP due JTF J3		
1800	2300	J1 VTC with Components		
1900	0000	JOC Shift Change and Update Brief		
2000	0100	SITREP Transmitted		
2100	0200	Shift Change Brief JFACC VTC		
2200	0300	JTF SITREP due to higher HQ CJTF JAC Update		
2300	0400	Chief of Staff Update		
0000	0500	Public Affairs Update		
0100	0600	Plans Synchronization Meeting		
0200	0700	J2 VTC with Components		
0300	0800	ROE/Force Protection Meeting		
0400	0900	J3 VTC		
0500	1000	CJTF Staff Brief		
0600	1100	CJTF Call with higher HQ		
0700	1200	JTCB Meeting		
0800	1300	J4 VTC with Components		

The "daily operations cycle" is synonymous with "battle rhythm." To ensure information is available when and where required, the JTF daily operations cycle is essential. All JTF staff, components, and supporting agencies should participate in the development of the daily operations cycle. The JTF chief of staff should be the approval authority for changes. When establishing the daily operations cycle, the JTF HQ should—

a. Monitor the daily operations requirements of higher HQ.

b. Ensure all subordinate daily operations cycles meet the needs of the JTF.

c. Monitor for conflicting JTF requirements (particularly for key personnel).

d. Keep changes to a minimum.

8. Reports Development

Standardized reports help reduce the amount of staff work to meet recurring information requirements. Table III-3 contains some sample reports, requests, and orders for which the JTF and components may be responsible. The table provides a brief description of the report, the sender, receiver, and when and how to transmit. This matrix organizes reports according to the responsible directorate. The matrix reflects the following information:

a. Report title: Report title or type of information provided.

b. Submitted by: The component or agency normally responsible for submitting the report to the JTF.

c. Submitted as of: Close out time for recurring reports. This should be within no more than one hour of the arrive NLT time.

d. Arrive NLT: Time to post the report for JTF review.

e. Transmission Type: System used (such as e-mail, AUTODIN, and so forth).

f. Precedence: The precedence to use when notifying the JTF the report is available (not applicable to some notification methods).

g. Addressee: Who the report goes to.

h. Info to: Additional addressees.

Table III-3. JTF Reports Matrix

Report Title	Submitted by	Submit as of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
Personnel Status Report	Components	2000Z	2100Z	E-mail Home page	Routine	JTF J1	
Casualty Spot Report	Components	As Required	As Required	E-mail	Routine	JTF J1	
EPW/CI/DET Report	Components	2300Z	2400Z	E-mail	Routine	PM	JTF J2
Intel Requests for Information (RFI)	Components	As Required	As Required	COLISEUM	Priority	JTF J2	

Table III-3. JTF Reports Matrix

Report Title	Submitted by	Submit as of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
Captured Material Report	Components	As Required	As Required	E-mail	Priority	JTF J2	
Component INTSUM	Components	0500/1700Z	0600/1800Z	JDISS	Routine	JTF J2	Components
Spot Reports	Components	As Required	As Required	E-mail	Routine	JTF J2	
JTF Recon 2	JTF J2	As Required	As Required	AUTODIN, JDISS	Priority	Combatant Cdr	Components
Component Recon 3	Components	As Required	As Required	AUTODIN, JDISS	Priority	JTF J2	Combatant Cdr
Component Recon 4	Components	As Required	As Required	AUTODIN, JDISS	Priority	JTF J2	Combatant Cdr
JTF DISUM	JTF J2	2200Z		Home page AUTODIN	Routine	Combatant Cdr	Components
JTF Graphic Supplement	JTF J2	1000/2200Z		Home page	Routine	Combatant Cdr	Components
Component INTSUM w/ Graphic Supplement	Component J2	0800/2000Z		Home page JDISS	Routine	JTF J2	
Collection Emphasis Message	Component J2	Last 24 hrs		Home page AUTODIN	Routine	JTF J2	
JTF Collection Emphasis Message	JTF J2	Last 24 hrs		Home page AUTODIN	Routine	Combatant Cdr	Components
SITREP (CDRs Situation Report)	Components	2400Z	0100Z	AUTODIN/ Home page	Priority	CJTF, J3	Components
JTF CDR SITREP	JTF J3	1000/2000Z	1000/2000Z	AUTODIN/ Home page	Priority	Combatant Cdr	Components
Orders (FRAGO, WARNORD, OPORD)	JTF J3	As Required	As Required	AUTODIN/ Home page	Priority	All	Components
RFIs (except Intel)	Components	As Required	As Required	E-mail	Priority	JTF RFI Manager	
RFIs (except Intel)	JTF RFI Manager	As Required	As Required	Home page	Priority	Combatant Cdr	
Engagement Status	Components	As Required	As Required	E-mail	Priority	JTF J3 ADA	Components
SAM Report	Components	As Required	As Required	E-mail	Priority	JTF J3 ADA	Components

Table III-3. JTF Reports Matrix

Report Title	Submitted by	Submit as of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
Significant Event Spot Report	Components	As Required	As Required	E-mail	Priority	JTF J3 ADA	Components
Daily Targeting Guidance MSG	JTF J3	1200Z	1300Z	Home page	Priority	Components	JTF STAFF LNOs
Target Report	Components	Continuous	Continuous	E-mail	Priority	JFACC JIC	JTF J3
Target Bulletin	J3	Continuous	Continuous	E-mail	Priority	Components	Combatant Cdr
Daily PSYOP Report	Components	2400Z	0100Z	E-mail	Priority	JPOTF/J3	Components
PSYOP Spot Report	Components	As Required	As Required	E-mail	Priority	JPOTF/J3	Components
NBC 1	Components	As Required	As Required	Voice, E-mail	Flash	JTF NBC	Components
NBC 2	Components	NLT 2 hours after '"As of time"	As Required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 3	Components	As Required	As Required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 4	Components	As Required	As Required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 5	Components	After Survey Completed	As Required	GCCS E-mail	Immediate	JTF NBC	Components
NBC 6	Components	When requested	When requested	GCCS E-mail	Immediate	JTF NBC	Components
LOGSITREP	Components	0600-0600 L	1000 L	Home page	Routine	JTF J4	
LOGSITREP	JTF J4	0600-0600 L	1800 L	Home page	Routine	Combatant Cdr	Components
Munitions Report	Components	0600-0600 L	1000 L	Home page	Routine	JTF J4	
Bulk Petroleum Contingency	Components	0600-0600 L	1000 L	Home page	Routine	JTF J4	
Munitions Report	JTF J4	0600-0600 L	1800 L	Home page	Routine	Combatant Cdr	Components
Bulk Petroleum Contingency	JTF J4	0600-0600 L	1800 L	Home page	Routine	Combatant Cdr	Components
Environmental Status	ARFOR	Weekly		Home page	Routine	J4	
Engineer SITREP	Components	2400/0800Z	0100/0900	Home page	Routine	J4	

Table III-3. JTF Reports Matrix

Report Title	Submitted by	Submit as of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
Engineer Compatible Report	Components	As Required	As Required	Home page	Routine	J4	
Civil Affairs Daily Report	Components	2400Z	0100Z	E-mail	Routine	JCMOTF	Components
Civil Affairs Spot Report	Components	As Required	As Required	E-mail	Priority	JCMOTF	Components
CA Resource Report	Components	2400 Local	0100	E-mail	Routine	JCMOTF	Components
Civil Affairs Report	Components	2400Z	0100Z	E-mail	Routine	JCMOTF	Components
Dislocated Civilian Report	Components	2400 Local	0100	AUTODIN/ Home page	Routine	JCMOTF	Components
Legal Report	Components	2400Z	0100Z	AUTODIN	Routine	JTF SJA	Components
Public Affairs Report	Components	1800 Local	1900 Local	AUTODIN/ Home page	Routine	JIB JTF PAO	
Religious Ministry Spot Report	Components	1200 Local	1300 Local	E-mail	Routine	JTF Chaplain	
Medical Spot Report	Components	As Required	As Required	GCCS E-mail	Priority	JTF Surgeon	
Medical Status Report	Ech III Med Fac	2359 Local	0100	GCCS E-mail	Routine	JTF Surgeon	JTF J4
Medical Survey	Ech III Med Fac	Weekly		GCCS E-mail	Routine	JTF Surgeon	JTF J4
Blood Report	Blood Unit	2359 Local	0100	GCCS E-mail	Routine	JTF Surgeon	JTF J4
Medical Supply Status	SIMLM	2359 Local	0100	GCCS E-mail	Routine	JTF Surgeon	JTF J4
Medical Regulation	Ech III Med Fac	As Required	As Required	GCCS E-mail	Priority	JMRO	JTF J4
Air Evac Request	Air Evac Request	As Required	As Required	HF Secure	Priority	AECC	
Air Evac Response	Air Evac response	As Required	As Required	HF Secure	Priority	AELT	
Air Evac Confirmation	Air Evac confirmation	As Required	As Required	HF Secure	Priority	AECC	
MIJI	Components	As Required	As Required	E-mail	Immediate	JTF J6 J3 J2	Components

Table III-3. JTF Reports Matrix

Report Title	Submitted by	Submit as of	Arrive NLT	Transmission Type	Precedence	Addressee	Info To
Frequency Interference Report	Components	As Required	As Required	E-mail	Immediate	JTF J6	Components
Comm Spot	Components	As Required	As Required	E-mail	Priority	JTF J6	Components
Comms Status Summary Report	Components	2400z	0100Z	E-mail	Routine	JTF J6	
Comms Status Summary Report	JTF J6	2400Z	0100Z	E-mail	Routine	Combatant Cdr	Components
Bead Window Report	Components	As Required	As Required	E-mail	Immediate	JTF J6	Components

9. Orders

The CJTF issues guidance and direction in the form of WARNORD, FRAGOs, execute orders, operation orders (OPORD), and other directives. The JTF JOC is the focal point for disseminating orders. The JTF IMP must address procedures for the management of plans and orders throughout their life cycle to include, distribution, acknowledgement, and protection.

10. Briefings and Meetings

a. Briefings and meetings. Both can be the biggest time consumer for JTF members if they are not conducted properly. Meetings should occur to accomplish a specific purpose, on an as-needed basis. The following are some representative meetings, with suggestions on their conduct. This is not an all-encompassing list. There are three roles that need to be specified for all meetings. The meeting organizer schedules the meeting, and publishes the agenda. This agenda will specify the attendees, purpose of the meeting, and desired outcomes of the meeting. The moderator is the person who runs the meeting, gathers input, and assigns tasking during the meeting. The final role is that of the recorder, who acts as the scribe, and at the end of the meeting, reads back all taskings to include who was tasked. The COS determines which meetings occur via the published JTF battle rhythm.

b. CJTF daily update brief. The CJTF daily update brief (see tables III-4 and III-5) is normally conducted once daily to update the commander on current operations, future, and long range plans. However, the update briefing can also be conducted as required. The update briefing's purpose is to provide the CJTF with analyzed information essential for decisionmaking and synchronizing the efforts of the JTF. A secondary purpose is efficient cross leveling of information within the staff. Brevity, clarity, and a cross-functional analysis of the battlespace are the goals of the CJTF brief. The most common error occurring in the daily update brief is that the focus is purely on what happened, vice the future. JTF commanders and staffs should ensure their update briefs remain focused on the future, rather than the past.

Table III-4. Recommended CJTF Briefing Slides (others added, as required)

Slide Title	*Responsibility*
Current C/D-Day	J3
Current operational phase	J3
Current operations situation assessment	J2/J3
Significant activities	J2/J3
ATOs (current, next 24 hours, next 72 hours)	JFACC
Future operations in planning	J3/J5
Sequels/transition plans in planning	J5

(1) Recommended briefing slide preparation.

(a) Establish an approved standard briefing format. The following are guidelines for creating a standard format:

- Use black letters on a white background for contrast and ease of reading.
- Use no more than 7 lines of text per slide.
- Keep graphics simple.
- Do not use animation effects.

(b) Store approved standard briefing format file on a shared network drive.

(c) Slides will be updated prior to the scheduled brief.

(2) Post a copy of the daily update brief to the home page. Include a summary of taskings that arose from the meeting.

Table III-5. Suggested Briefing Sequence (other personnel added, as required)

Briefing	*Responsibility*
Introduction	J3
Fused J3/J2 current operations update	J2/J3
Targeting/air tasking order (ATO) update	J3 Air
Future operations plans	J3/J5
Long range plans	J5
C4 update	J6
As required	Special staff
Issues	Component LNO
Issues	COS
Conclusion	J3

d. Plans synchronization/integration meeting. Recommend the future plans officer chair a daily plans synchronization/integration meeting. The purpose is to ensure future and long-range planning efforts are synchronized and integrated with the current operational situation, and prioritizing supporting branch plans in accordance with the current situation. Representatives from J2, J3 current operations, J5 plans, and staff directorates should attend the meeting.

11. Internal Policies and Procedures

a. Defense message system (DMS)/AUTODIN messages.

(1) The JOC monitors incoming message traffic and posts messages to an incoming message web site, etc. Track messages by the date-time-group (DTG), originator, subject, or key words describing message content. Using an approved joint message handling system or other spreadsheet/automated message handling service (AMHS)/web page similar to the example in table III-6, users can use a "FIND" command to locate messages related to a subject or key word reference.

(2) Each directorate establishes internal message handling procedures to manage incoming and outgoing messages on the appropriate web page.

(3) The IMP should address DMS/AUTODIN message procedures to include release authority, hardcopy, and softcopy requirements, and DTG assignments.

Table III-6. Sample JOC Message Log

DTG	*ORIGINATOR*	*SUBJECT*	*KEYWORDS*			
141752Z JUN 98	CDRUSJFCOM/J3	WARNING ORDER				
171420Z JUN 98	CDRUSJFCOM/J3	WARNING ORDER TWO	TASKINGS	CCIR		
181839Z JUN 98	CDRUSJFCOM/J3	WARNING ORDER THREE	JTF 780	INTENT		
190900Z JUN 98	CDRUSJFCOM/J3	PLANNING ORDER (PART ONE)	PLANNING GUID.	TASKINGS	FORCES	IW FOCUS
191910Z JUN 98	CDRUSJFCOM/J3	PLANNING ORDER (PART TWO)	LIFT ALLOCATION	CCIR	LOGISTICS	
191530Z JUN 98	CJTF 780	WARNING ORDER NUMBER ONE	COMPONENTS	COMPONENTS	MISSION	INTENT
192042Z JUN 98	CJTF 788	EXTEND BOUNDARIES OF JOA	JOA	JSOTF		
201345Z JUN 98	CJTF 788	CONTROL OF PSYOP/CA	PSYOP	CIVIL AFFAIRS	C2	
201610Z JUN 98	CTF 785	KEY PERSONNEL LISTING	C2	PHONE		
201810Z JUN 98	CTF 785	JOA MODIFICATION	JOA			
202200Z JUN 98	CJTF 780	WARNORD TWO	TENTATIVE COAS	PLANNING GUIDE	DEPLOYED HQ.	
211524Z JUN 98	CTF 785	CARRIER AIR WING MODIFICATION	AIR WING			
211830Z JUN 98	CTF 785	REQUEST FOR MIGRANT VESSELS	MIGRANTS			
212320Z JUN 98	CTF 785	CHOP COGARD FORCES	COGARD	MIGRANTS		
221306Z JUN 98	CJTF 780/J3	FRAGO ONE	AFFOR	ISB		
231700Z JUN 98	CJTF 788	COURSE OF ACTION (CONOPS)	PHASES	JSOTF	CONOPS	
231720Z JUN 98	CJTF 788	PATROL CRAFT TACON SHIFT	COGARD		JSOTF	
232035Z JUN 98	CJTF 788	MESSAGE CORRECTION	231700Z JUN 96	JSOTF	CONOPS	
241226Z JUN 98	CTF 785	ASSIGNMENT OF COGARD & USN	JTF X	COGARD	USN	
241426Z JUN 98	CJTF 780	FRAGO TWO	MIGRANT CAMP	CVBG	MEU/ARG	JFMCC
280257Z JUN 98	CJTF 780	PLANNING INFORMATION	ROCK DRILL	FDESC		
280335Z JUN 98	CJTF 780	FORCE DEPLOYMENT EXERCISE	DEPLOYMENT			
281910Z JUN 98	CTF 789	JFACC/AFFOR BBS	JFACC	AFFOR	ACP	ACO
282157Z JUN 98	CJTF 780	INTENT FOR IW IN PHASE III	IW	PHASES		
300115Z JUN 98	CTF 783	REQUEST FOR GUIDANCE	FOB	SAR	MEU	TMD
011844Z JUL 98	CJTF 780	SOTA REQUEST CHANGE ONE	SIGINT			
011600Z JUL 98	CTF 785	OPERATIONS TASK SUBMISSION	JFMCC			

(4) Staff directorate duties include message review, reading files, suspense assignment, and coordinating activities. Suspense control procedures consist of assigning, copying for distribution, and reviewing status. Maintain a message log for both incoming and outgoing messages.

(5) Each directorate is responsible for maintaining copies of outgoing/incoming correspondence and suspense items. Submit messages through the appropriate staff director or the JTF COS for release. Provide the drafter a comeback copy of all approved and released outgoing messages. The COS reviews the outgoing messages requiring CJTF and JTF review.

b. Master suspense action log. The JOC maintains a suspense log of all taskers received (see table III-7). The JOC chief assigns an OPR and office(s) of collateral responsibility (OCR), and forwards to the OPR and OCR for action. The master suspense action log contains the following entries: tasking agency, OPR, OCR, suspense time, close out time, and a brief summary of the tasking. The following instructions apply to the sample master suspense action log:

(1) Action Item: The message (MSG) or article establishing a JTF task or requirement.

(2) Received: DTG the JOC receives the tasking.

(3) Tasked by: Originator of the tasking. Unless otherwise directed, submit responses to the originator.

(4) OPR: The JTF directorate or staff agent responsible for completing the tasking.

(5) OCR (office of collateral responsibility): The JTF directorate or staff agency assigned to assist the OPR in completing the assigned tasking.

(6) Suspense: DTG to complete the tasking and post the results to the originator.

(7) Close Out: Actual completion DTG of the tasking.

(8) Task Description: Brief description of the tasking.

Table III-7. Sample Master Suspense Action Log

ACTION ITEM	*RECEIVED*	*TASKED BY*	*OPR*	*OCR*	*SUSPENSE*	*CLOSE OUT*	*TASK DESCRIPTION*
MSG 190337Z FEB 97	192330Z FEB 97	CDRUSAREUR J3	J3	J4	221200Z FEB 97		IDENTIFY FORCE REQUIREMENTS FOR RAMP UP TO 56,000 MIGRANTS
NG 02/19/97 1536	191536 FEB 97	CDRUSAREUR J4	J4		192400Z FEB 97	192259Z FEB 97	STATE EXPECTED CONSUMPTION RATE OF CLASS I
MSG 201128Z FEB 97	201430Z FEB 97	CDRUSAREUR J3	J3		211200Z FEB 97	211132Z FEB 97	DEVELOP COAS FOR SEVERE WEATHER EVACUATION
	181320Z FEB 97	CDRARLANT J2	J2		19 1200Z FEB 97	191200Z FEB 97	REQUEST CONSIDER ALTERNATIVES FOR MIGRANT TREATMENT BY DOD AND NON DOD PERSONNEL
NG 02/19/97 0334	190338Z FEB 97	CDRARLANT J4	J4		201200Z FEB 97	201002Z FEB 97	REQUEST FOR LAYOUT OF MIGRANT AND JTF CAMP, REQUEST COA FOR DESTRUCTIVE WEATHER RELOCATION
NG 02/19/97 1826Z	191832Z FEB 97	CDRARLANT CAT	J4				ASSESS FACILITIES AVAILABLE ON NAVBASE FOR HURRICANE (CAT I) PROTECTION

c. JTF significant events log. Table III-8 is an example of an official chronological account of the activities of a JTF. The significant events log is a running account of JTF significant events. The JOC maintains the log. Instructions for completing the sample log are as follows—

(1) Time. The time JOC notes or receives a report of the event.

(2) Notified. Key personnel the JOC chief notified.

(3) Event Description. A brief description of the event. If a follow-on report, refer to DTG of original report.

Table III-8. Sample JTF Significant Events Log

TIME	*NOTIFIED*	*EVENT DESCRIPTION*
121300Z FEB 97	CJTF, Chief of Staff	JCS WARNING ORDER DIRECTING CDRSOUTH TO BEGIN MIGRANT OPS PLANNING
180300Z FEB 97	CJTF, J3	CDRSOUTH ACTIVATES JTF 160 AND DIRECTS COMMENCEMENT OF MIGRANT OPS
181240Z FEB 97	J3, J4	M/V ELVA II STRUCK PILINGS ON CALLAN RR BRIDGE. JAX HARBOR CLOSED TO ALL TRAFFIC UNTIL FURTHER NOTICE
181348Z FEB 97	CJTF, J4	PRE-STAGED RATIONS AND WATER SUPPLIES HAVE BEEN CONTAMINATED. CURRENT SUPPLY LEVELS ESTIMATED AT 10 DAYS.
191210Z FEB 97	CJTF	ATTEMPTED MURDER AND RAPE IN CAMP ALPHA
191624Z FEB 97	J4	COMNAVSTA IMPLEMENTS WATER RATIONING PROCEDURES
200405Z FEB 97	CJTF	FIRE IN MIGRANT VILLAGE CAMP ALPHA, 3 MIGRANTS SEVERELY BURNED FIGHTING FIRE. FIRE EXTINGUISHED BY CAMP FIRE TEAM AND NAVSTA FIRE DEPARTMENT AT 0630Z

d. JTF phone and e-mail directory. The JTF and components J6 or equivalent should publish a phone and e-mail directory (preferably on the JTFs web site on the SIPRNET). The directory contains a brief description of available communications means, instructions on use, and a list of staff functions with telephone numbers and e-mail addresses. Publish the directory on an appropriate electronic medium (that is, local area network, web page, etc.). Table III-9 contains a sample directory listing.

e. Records management. Establish a records management program for managing information throughout its lifecycle. The J6 has responsibility for establishing the program and appointing the JTF records manager. For more details on records management responsibilities, policies, and procedures, see DODD 5015.2, CJCSI 5760.01; CJCSM 5760.01,Vols 1 & 2; and, for an example, appendix B of this publication. Functional and service components use their own records management publications for setting up and managing their programs.

f. Mail and publications. Some organizations have unit mailrooms, and publications and forms under the responsibility of the J1, while others have them as J6 responsibilities. In either case, they have an impact upon the JTFs IMP and should be addressed accordingly.

Table III-9. Sample JTF Telephone and E-mail Directory

BILLET/USER	*DEVICE*	*SECURE YES/NO*	*DSN*	*COMMERCIAL*	*TACTICAL*	*E-MAIL*	*REMARKS*
JTF 780							Home Page http://JTF780
CJTF	STU-III FAX DSVT	Yes Yes No	836-6545 836-6332	(757) 322-6545 (757) 322-6332	201-4201-850	J00	
DCJTF						J01	
CHIEF OF STAFF						J00COSf	
J1							
J2							
J3							
J4							
J5							
J6							
COMMANDER	STU-III FAX DSVT DNVT	Yes Yes No No			201-4201-241 201-4201-242		
ARFOR							Home Page http://ARFOR
MARFOR							Home Page http://MARFOR
AFFOR							Home Page http://AFFOR
NAVFOR							Home Page http://NAVFOR

12. Multinational Procedures

a. The JTF establishes procedures for data transfer between the JTF, multinational components, and other agencies. The JTF establishes a multilevel security (MLS) concept of operation for the specific "how-to" for data transfer. Develop information sharing/disclosure policies in accordance with DOD and/or approved multinational policy or procedures. Handle multinational procedures for transferring data dealing with sensitive compartmented information through SSO channels.

b. Coalition wide area network (CWAN) (CENTRIX) employment. CJTF 180 has used CENTRIX in Operation ENDURING FREEDOM.

(1) CENTRIX is a coalition wide area network (CWAN). It provides a network classified at COALITION SECRET on which coalition staff officers may operate.

(2) Coalition partners draw information from CENTRIX via web, email or file transfer. CENTRIX resides on its own network, so users within the CENTRIX system may operate as on any other network.

(3) The CJTF 180 knowledge and information management plan (KIMP) (http://www.acc2langley.af.smil.mil/alsa/CJTF180KIMP.pdf) has more detail regarding CENTRIX procedures.

Chapter IV
INFORMATION SYSTEMS

1. Background

The goal of information systems and IM procedures is to produce an accurate picture of the battlespace and supporting decisionmaking. Information systems must provide effective and secure information exchange throughout the JTF. Table IV-1 provides a summary of information systems currently available. Users need to develop an understanding of the information systems available and IM procedures to match their information requirements.

Table IV-1. Common Information Systems

SYSTEM	*VISIBILITY*	*USES*	*SIMILAR TO*	*PURPOSE*	*AVAILABLE AT*
GCCS (COP)	-Sender & Receiver in GCCS Community	-Official, For record E-mail -Updating the COP -Formal Traffic -Conducting Dialogue and Coordinating Actions	-Telephone or Conference Call -Coordinating Official Actions -AUTODIN -Web Pages	-One to One -One to Many -Smart Push or User Pull	-JTF HQ -Subordinates -Some JTFs
COLISEUM	- Available to SIPRNET and JDISS Community	- Requests For Information Management	-Discussion of Issues at local, regional and global level -Receiving Staff Input	-One to Few -One to Many -Many to Many	-JTF HQ -Some MILGps and JTFs
JWICS	-Available to SCI users only	-E-mail, VTC -SCI web browsing -SCI file transfer -SCI chat -SCI collaboration	-NIPRNET and SIPRNET, but at SCI level	-One to One -One to few -One to Many -Many to Many	-JTF HQ -Component HQs -Unit levels to organizations requiring SCI access
WebPages/ Portals	-Available to SIPRNET and NIPRNET Community -Commercial Internet Availability	-Information for record, Messages, News -COAs, OPLANs -RFIs -Other final products -Official Positions, decisions -General Information	-Publishing a Newspaper -One Stop Shopping	-One to Many -Many to Many -Smart Push or User Pull	-JTF HQ -Subordinates -Some MILGps and JTFs
E-mail	-Sender & Receiver -Classified or Unclassified Availability	-Informal/Formal dialogue -Resolving and Negotiating -Private or Group Recipients -External File Transfer	-Telephone or Conference Call -Informal Memorandum	-One to One -One to Many	-JTF HQ -Subordinates -MILGps -Available thru multiple sources, i.e., LAN/WAN, GCCS, CNCMS, SIMS
Collaborative tools/DCTS	SIPRNET	-Voice and chat services -Whiteboard collaboration -VTC conferencing -Threaded discussions	-Net meeting	-One on One -One to Many	-JTF HQ -Subordinates -Other Commands and components
LAN/WAN	-All LAN/WAN Capable Users -Classified (LIMS/SIPRNET) or Unclassified (NIPRNET) Availability	Staff coordination Working document management Local SOPs, Schedules, Calendars, etc. Internal File Transfer Transfer from other sources, i.e. GBS	-Circulating Written Drafts for Review and Coordination -Discussion of Local Issues -Receiving Staff Input	-One to Few -One to Many -Many to Many	-JTF HQ -Subordinates -Other Commands and Components

Table IV-1. Common Information Systems

SYSTEM	*VISIBILITY*	*USES*	*SIMILAR TO*	*PURPOSE*	*AVAILABLE AT*
VTC	-Available to SIPRNET, JWICS and NIPRNET Community	-Informal/Formal Voice Dialogue -Resolving and Negotiating -Individual or Few Recipients	Telephone or Conference Call Coordinating Official Actions	-One to Few -One to Many -Many to Many	-JTF HQ -Subordinates -Some MILGps and JTFs
Organizational Message	-All AMHS/DMS Capable users -Classified or Unclassified Availability	Inter-organizational Official Communication -Transmission of Orders, Reports, Plans, Intelligence -General Service Written Communication	-Official E-mail -Hardcopy mailing of documents	-One to One -One to Few	-JTF HQ -Subordinates -Some MILGps and JTFs
GBS	-SIPRNET -NIPRNET	-Wide area file dissemination	-Direct TV	-Many to Many	-All components in coverage area
IDM	-SIPRNET -NIPRNET	-Information cataloging -File search -Content staging -Product profiling		-One to Many -Many to Many	-JTF HQ -Some combatant commanders -Subordinates
Voice-(DRSN, STU-III, UHF TACSAT, MILSTAR)	-Sender & Receiver -Non-Secure & Secure	-Informal/Formal Voice Dialogue -Resolving and Negotiating -Individual or Few Recipients	-Standard Telephone -Conference Call	-One to One -One to Few -Few to Few	-JTF HQ -Subordinates -Government Agencies

2. Global Command and Control System

a. GCCS is one of the IM systems used by a JTF. GCCS is a comprehensive, worldwide system providing information processing and dissemination capabilities necessary to conduct C2 of joint forces. This system improves visibility of the operational environment and, with commonly understood procedures, enhances situation awareness. There are four primary software modules within GCCS providing critical information flow to enhance situation awareness. They are the Joint Operations Planning and Execution System (JOPES), JDISS, COP, and a software package with a browser application program with e-mail capabilities. Basic descriptions of each module follow:

(1) JOPES. JOPES supports military planning, deployment, execution, redeployment, and operations monitoring. JOPES incorporates policies, procedures, personnel, and facilities by interfacing with automated data processing systems and reporting systems providing support to senior level decision makers and their staffs with the capability to plan and conduct joint military operations. (For example, JOPES is used to submit movement requirements to United States Transportation Command [USTRANSCOM].) Information regarding crisis action planning is contained in CJCSM 3122.01, JOPES Volume I, chapter V. Specific guidance for the format and content of operations plans/orders are provided in CJCSM 3122.03, JOPES Volume II, enclosure C. No joint policy guidance exists for an IM appendix to annex K. Recommend users follow appropriate command or Service policy.

(2) JDISS. JDISS is a transportable workstation and communications system electronically extending a theater JIC to a JTF or other tactical users. JDISS requires a common SECRET Internet Protocol Router Network (SIPRNET) or Joint Worldwide Intelligence Communication System (JWICS), depending on classification. SIPRNET

supports secret information requirements. JDISS is the primary source for intelligence reporting, database access, access to the intelligence RFI system: COLISEUM. JDISS provides automation to pull information from other theater and national intelligence databases.

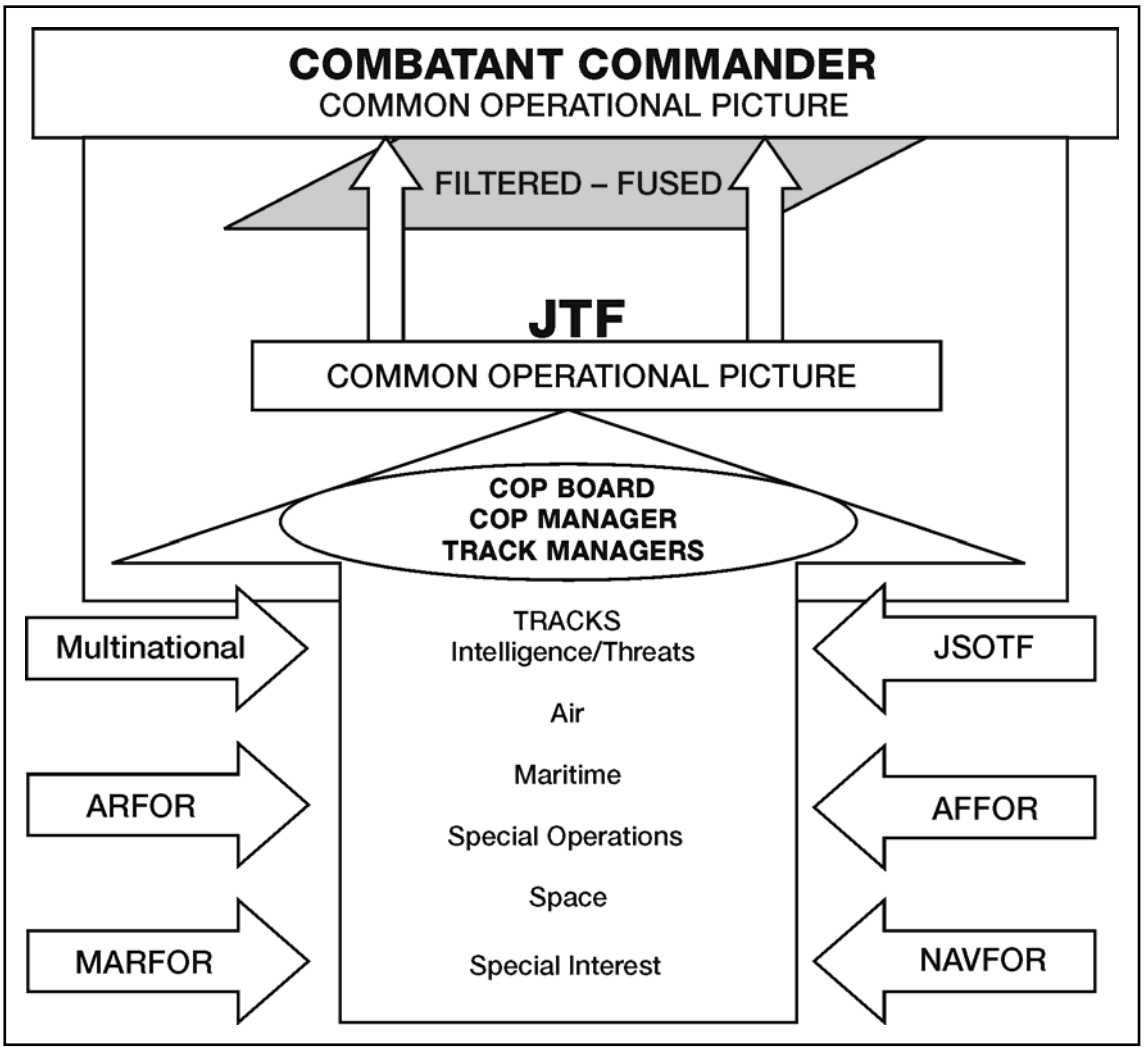


Figure IV-1. COP Flow Chart

(3) COP. Figure IV-1 depicts a skeleton outline of the COP process. The development and maintenance of the COP requires the JTF and all components adhere to established COP procedures and the procedures explained in chapter III. The JTF feeds the combatant commander's COP. Component reporting systems provide friendly and threat air, maritime, and ground locations/tracks. The COP provides commanders with a force tracking mechanism.

(4) Software package. Currently, GCCS uses a browser application program to provide e-mail, and other capabilities.

b. The Services have Service-oriented GCCS component systems that may present interoperability issues to the JTF IMO. The JTF IMP should account for any potential problems. These systems are—

(1) USAF: GCCS-AF.

(2) Army: GCCS-A.

(3) Navy/Marines: GCCS-M.

3. Joint Worldwide Intelligence Communications System

JWICS is a sensitive compartmented information (SCI)-secure, high-capacity, multi-media communications system that offers the military intelligence community a wide range of capabilities, including a secure video and audio service for both video telecasting and teleconferencing. The system also provides conventional network services for collaborative electronic publishing, the electronic distribution of finished intelligence, and tools to accommodate the transfer of reference imagery, maps, and geodetic materials, as well as other high-end graphics products.

4. Network Application Management

a. Networking technologies are expanding the options available for managing the flow of information. We can achieve a collaborative environment for sharing information using web pages, public folders, and e-mail. For example, networks provide the JTF access to nonsecure and secure information, allowing individuals to send and receive unclassified and classified information worldwide. The Nonsecure Internet Protocol Router Network (NIPRNET) provides access to the Internet. SIPRNET and JWICS provide access to classified information.

b. The intranet network infrastructure for a JTF HQ may differ from one JTF to another, but the concepts are generally the same. A JTF intranet is a communications network in which access to published information is restricted. The communication standards of the Internet and the content standards of the world-wide web (WWW) are normally the basis for a JTF intranet. Therefore, the tools used to create an intranet are normally identical to those used for Internet and web applications. Using LANs protected by firewalls, virtual private networks, intrusion detection systems, and demilitarized zones, a network administrator has the tools to establish a JTF intranet structure.

c. The JTF IMO must work closely with the JTF web administrator and the component IMOs to develop and establish procedures for LAN management. The JTF IMP should identify how the JTF shares information. The JTF IMO must establish procedures enabling each staff section to access, post, and update information. Each staff section ensures the information posted is accurate, current, and relevant.

d. Web sites and portals.

(1) A well-organized web site assembles, organizes, and presents vital information in a timely manner. The JTF HQ, staff directorates, components, and supporting agencies should develop and maintain their own web pages for the site. Information on these web pages should include, important updates, status reports, common staff products, and current activities.

(2) The JTF should organize the web site around a master "JTF home page." The JTF home page or "front door" sits at the top of the JTF web site acting as a point of entry into the site. In a complex JTF web site, it is impractical to populate the JTF home page with dozens of links. Complicated or large home pages are long and will not load quickly in a bandwidth-constrained environment. Therefore, each major element or unit of the JTF should have their own home page with direct links back to the JTF home page. However, a JTF home page could list (without links) URLs for other applicable JTF home pages to advertise their existence. Web pages or pages within a component should have a consistent design to facilitate navigation.

(3) The JTF must design the web site so users (at every workstation with a web browser) can quickly navigate regardless of where they enter the site. Ease of navigation, via links from any point on the site is important. All JTF web pages should include a basic set of links logically connecting them to other web pages on the site.

(4) Web pages are rapidly moving beyond a static presentation of information and are evolving into web portals. Portals are "smart" web pages that dynamically present tailored information based on the needs of the user and customer profiles. Examples of portals include the Army Portal, Army Knowledge Online, at https://www.us.army.mil/portal/portal_home.jhtml. Another portal available to combatant commanders is the information dissemination management (IDM) application being developed by the Defense Information Systems Agency (DISA).

e. Electronic mail (e-mail).

(1) E-mail is a highly effective means to communicate information, providing rapid dissemination of time critical information within the JTF. E-mail permits rapid and asynchronous communications, eliminating "telephone tag." It permits a single user to communicate with one or several users simultaneously. However, to reduce e-mail overloads, consider establishing functional versus individual accounts to avoid unnecessary e-mail overload. This helps prevent a message backlog for personnel not on shift. Additionally, development of a precedence system within E-mail identifies messages requiring timely handling and review.

(2) E-mail can overload the network if used improperly. Unnecessary information and large message attachments overload the network. Use web sites, public access drives, or send a link (vice the actual attachment) on the LAN to disseminate information. Remove graphics, imagery, and text documents that do not add information content. Develop graphics/briefing slides relying on few colors since not all users have access to color printers.

(3) At times, it is necessary to notify a large audience that a particular piece of information is available (for example, warning orders). Users should use some discretion in selecting e-mail addressees. In most situations it is preferable to send a link to the information and notify intended recipients where it may be retrieved, vice attaching the item to multiple e-mail messages. This procedure reduces the bandwidth used when sending multiple copies of e-mails with attachments. Users should periodically review their e-mail group addresses for accuracy and ensure topic-related group members are still current. Remember, undeliverable mail may double the network load (once to attempt delivery and again to notify the sender of the delivery failure). Users should take prompt action to resolve the cause of undeliverable e-mail.

(4) Although e-mail is an effective means of communications, users within a JTF need to keep in mind certain rules and follow protocols to ensure the electronic medium remains effective. E-mail etiquette is essential. Some example digital rules of protocol are presented in appendix D.

f. Shared disk drives and folders are another means to allow common access to information. Organizations using shared drives should have an established policy for deleting obsolete and outdated information. Shared drive folder names may be topical or use the same titles as those shown in the file plan drive. An example of topically named shared message folders is in table IV-2. A sample file plan drive setup is shown in figure B-1.

Table IV-2. JTF Shared Message Folders

J1	*J2*	*J3*	*J4*	*J5*	*J6*
Admin	Action Items	Air Ops	Briefings	Briefs and Slides	Admin
Completed Taskers	Admin	Airlift	General Info	Force Protection	Directories/Rosters
Daily News Briefs	JULLS	Fighters	RFI	J1	Organization Structure
Incoming Messages	MSG-Air	Army Aviation	Play-Info	J2	Briefing Slides
Need Information Requests	MSG-BDA	Army Ground	Reports	J3	Incoming Messages -COMSTAT -SITREP
Outgoing Messages	MSG-Force Protection	CMOC	Admin	J4	Outgoing -COMSTAT
Personnel	MSG-Ground	Everybody Read	Civil Engineers	J5 Staff	MESL -Incoming -Responses
SITREPS	MSG-IIR/Collection Report	EWO	Comptroller	Media	JULLS
J1 Reports	MSG-INSUM	General Info	Contracting	Taskers	Admin
Personnel Status Request	MSG-Naval	Info Ops	Director	RFI	Computer System Support
Receipts (Verification)	MSG-Political	JOC	Fuels		Current Ops
Policy Guidance	MSG-Refugees/Med	JULLS	LNO		FRAG Management
Postal	MSG-SITREPS	LNOs (J1, J2, J3, J4, J5, J6	Medical		Future Ops
Incoming	MSG-Targets	MSEL Events	Plans		Future Plans
Outgoing	MSG-Terrorist Activity	Navy Ops	Services		J6
Suspense's	MSG-Warning/Execute Order	Ops/Plans	Supply		JCCC
	WMD/NBC/SCUDS	Ops-Analysis	Suspense's		Joint Key MANAGEMENT
	Weather	Orders	Taskers		Joint SYSCON
		FRAGOS	Transportation		JULLS
		Warning Orders	Weapons		LNO (DISA)
		PSYOP	JULLS Inputs		Networks
		RECCE	Maintenance		Policy Guidance
		SITREP Inputs			Refugee Evacuation Procedures
		SITREPS			Rhythm
		SOF			SITREP Inputs
		Special Staff			
		JOPES			
		Space			
		Taskers			
		TMD			

g. The workflow management process implements electronic distribution of work. This definition emphasizes two important ideas about workflow. First, workflow must reflect the true business practices and procedures of an organization. In other words, a workflow must be able to capture the WHO, WHAT, WHEN, WHERE, and HOW of an organization, and use them to control flow and distribution of work. Secondly, workflow must control the flow and distribution of work electronically. Along with electronic packaging and

coordination, electronic workflow products provide the capability to suspense and track correspondence throughout the workflow process and provide action officers and document originators status concerning their packages.

h. Document management is a process that facilitates the acquisition, classification, storage, and access of organizational documents. Document management is concerned with maintaining and organizing the electronic information introduced during the workflow process, as well as other documents introduced outside of the workflow process. This is done by managing documents in central locations, controlling access to these files, keeping a history of activity and changes to the managed documents, and allowing users to search for documents. This centralization allows collaboration between individuals and groups, with the application keeping track of all of the users accessing the documents and any modifications they might make.

i. Document properties must be captured to effectively manage documents in a records management application. These properties should be in compliance with the standards laid out in the DOD joint technical architecture. As such, several document management requirements have been incorporated into DODD 5015.2-STD.

j. Records management application (RMA) is a system that provides services to categorize, store, locate, retrieve, and dispose of electronic records. It is concerned with storing electronic records to comply with all legal and regulatory requirements. Similar to document management, metadata (data about the document) is collected from the system and users. The system stores this metadata along with the record in such a manner that it can be altered only by an authorized user: a key legal requirement for records management. Another key feature of a RMA is record disposition. Every record must be assigned a disposition that determines how long the record must be maintained and when it is ready for destruction or permanent storage.

(1) An RMA provides the records manager or his designee the capability to assign a selected list of file codes that a particular office or user would be permitted to use. The user would then select from this designated list where records would be filed. The selected list of file codes would then be the same group that the user accesses when searching for records needed. The system would provide the capability to allow the user to limit searches on the system and direct what files must be searched.

(2) Many commands have established guidance to structure shared drives, hard drives, etc., similar to office file plans and manage electronic information accordingly. Although this is a suitable system, it doesn't meet National Archives and Records Administration requirements or automatically ensure information is disposed of when it has served its purpose or has met required retention periods.

k. Electronic transaction system/publications library provides access to both electronic and physical publication/ forms and products, 24 hours a day, 365 days a year. Includes electronic repository, physical product distribution centers, order desk, and help desk. Unlike the DOD electronic publications/forms library, the Air Force's is only available on NIPRNET.

l. Standard office products applications support information life cycle management and along with electronic mail capabilities, provide the primary desktop avenues for creating, processing, and using information. They include word processing, presentation graphics, spreadsheets, database management, and electronic publishing tools.

5. Defense Collaborative Tool Suite/InfoWorkspace

a. The Defense collaborative tool suite (DCTS) is a standard for a set of personal computer (PC)-based systems, software applications, and tools designed to support JTF planning, decisionmaking, execution, and assessment. DCTS allows for video teleconferencing, voice-over-Internet protocol (IP) conference calling, digital whiteboarding, application sharing, instant messaging, and virtual meeting rooms. Current products that meet the DCTS standard can be found at: http://lyris@jitc.fhu.disa.mil/jit_info.htm. JTFs using DCTS must ensure their PCs are equipped with audio headsets that include boom microphones. WebCams may be used for specific users, but should be restricted in number due to bandwidth limitations.

b. DCTS promises to revolutionalize how collaboration is done within a JTF. In lieu of expensive, time consuming travel, JTF planners can hold virtual meetings over the Defense Information Systems Network (DISN). DCTS provides the means for one-to-many or many-to-many collaboration sessions over the DISN.

c. Collaborative tools can be used to bridge seams across an organization, such as between components separated by distance, or for elements within the JTF staff. The following are some examples of how to use such tools:

(1) Present an interactive visual projection enabling members of the JTF to see the collaborative effort both on their workstation screen and on a large "movie screen" display.

(2) Support the JTF planning process by permitting JTF planners to enter virtual meetings to share intent and build common planning documents.

(3) Provide products that enable a CJTF's daily briefing to be presented and shared throughout the JOA.

(4) Share and work on documents in real time between the JTF headquarters and subordinate components. These documents include force lists and availability, intelligence information, time phased force deployment data (TPFDD), worldwide map system, unit capabilities, equipment, organization for each Service (US), and other coalition forces as required.

d. Internet Relay Chat (IRC) is an interactive conferencing tool on GCCS, allowing users to open "chat channels" similar to that provided by DCTS. Chat channels permit one-to-one or one-to-many communications. Intended topics of discussion generally define communications channels. Typical IRC channels may be established for TPFDD developers and validators, information managers, etc.

e. SIPRNET Chat is a real time text-based application capable of a multi-point data exchange. Chat can be used to carry on interactive discussions among many individuals, or record meeting notes/action items discussed in a meeting and then the contents of the session can be saved for later review. Chat also allows any user to have a private side conversation with another person during a group chat session. By using abbreviations and various symbols (called emoticons), chat can convey emphasis and add emotional connotations to the discussion.

(1) Advantages.

(a) Chat is an immediate, dynamic, and synchronous discussion medium unlike e-mail that is a one-way static form of communication.

(b) The chat application consumes relatively low bandwidth.

(c) The chat application can be used to document discussion forums in a persistent form that can be stored as official records for later retrieval and reference.

(2) Disadvantages.

(a) Multiple conversations can occur simultaneously, which can cause confusion.

(b) Access is available to anyone unless control measures are used.

(c) Unconstrained use can strain limited bandwidth or cause server failures.

(d) Propensity for micromanagement.

(e) Experienced users frequently express thoughts in less than complete sentences and make extensive use of abbreviations, which may not be understood by all participants.

(3) Although the SIPRNET chat application is a very powerful tool for quick discussions among geographically dispersed parties, its use can easily be abused. The very strengths that make this tool so powerful can also render it useless unless formal management procedures are established.

(4) Because the chat application most closely resembles a radio network the same sort of procedural measures should be used. Suggested protocol measures include:

(a) SIPRNET chat use should be addressed in the communications plan – annex K, like all other communications networks.

(b) Guard charts should be used to define the chat network participant composition.

(c) Do not allow anonymous users. Access should be restricted to only pre-designated user accounts that coincide with the chat guard chart.

(d) Session leaders should be appointed to control the chat session and maintain the focus when multiple participants are involved.

(e) If abbreviations are used they must be standardized so everyone understands what they mean.

(f) Multiple chat conversations in one room can become very distracting; the session leader may limit the number of participants or send sidebar discussions to other chat areas.

(g) Private chat "rooms" (separate chat text windows) should be available for persons wanting to conduct sidebar discussions so they don't interfere with the main discussion.

(h) Virtual room logbooks should be saved (time and date stamped) at the end of each shift by the room custodian for future reference and to reconstruct chain of events as required.

6. Local Area Network/Wide Area Network

The JTF LAN can be set up with shared and/or private hard drive space. Private drive space is intended to limit access to stored data. Access is generally limited to specific functional areas, as defined by user login names (that is, specific joint-code staff sections). The shared or "public" drives are accessible by anyone given access by the LAN administrator. The public drives, organized with appropriate subdirectories, increase staff visibility of files and provide the opportunity for a larger staff audience (at one location) to coordinate, review, and approve staff issues. The LAN administrator establishes the shared drives. Staff sections are responsible for the currency, accuracy, and maintenance of their shared drive information.

7. Video Teleconference

a. The purpose of the JTF VTC capability is support of the JTF commander and his/her staff. VTCs are effective for sharing information and C2 between the CJTF and geographically dispersed subordinate commanders and staffs. While VTC is a key means of command and control, the JTF commander could use alternate methods of communication such as conference calls if a VTC system is not available. VTC provides—

(1) Verbal and visual communications.

(2) A communications medium to readily identify who is speaking.

(3) Visual queues (body language, etc.) missing with other forms of electronic communication.

(4) An alternate means of communication when travel for face-to-face meetings is either not available or inappropriate.

(5) Interactive information exchange between two or more elements.

b. Types of JTF VTCs.

(1) Reservation Based Service (DISN, digital video services–global (DVS-G)). This is the primary means of VTC between components and the JTF HQ for UNCLASSIFIED and up to Top Secret (TS) Collateral. Connectivity is either via IDSN or dedicated communications links between a JTF HQ and dispersed components.

(2) JWICS. JWICS VTC is the primary means of VTC involving SCI requirements.

(3) DCTS or InfoWorkspace. Either the DCTS standard or InfoWorkspace product can provide IP-based video connectivity over the NIPRNET or SIPRNET.

c. VTC concept. Reservation-based service and JWICS VTCs should be available for scheduling 24 hours a day except for required maintenance. The JTF battle rhythm dictates the schedule of the VTCs, and the JTF HQ is network control for the VTC. JWICS, DCTS, or InfoWorkspace are backups for the reservation-based video teleconferencing. The JWICS VTC is always located within a permanent sensitive compartmented information facility (SCIF) or a tactical SCIF (T-SCIF).

d. VTC procedures.

(1) GENSER VTC. Scheduling of the GENSER VTC is the responsibility of the organization desiring to set up the conference. The VTC scheduling manager works closely with the JTF IMO in developing the VTC schedule. The JTF commander is the primary

and priority user of this system. Components, staff directorates, and supporting agencies desiring to schedule a GENSER VTC submit their requests to the VTC scheduling manager. Prior coordination with the controlling SSO is mandatory for access to the JWICS VTS suite, especially for JWICS VTC participation by persons not indoctrinated for SCI. Coordination should include clearance and access verification for all participants who do not have routine access to the SCIF. The VTC scheduling manager should post the schedule at the location determined by the IMO and contained in the IMP. Prioritization for usage of the GENSER VTC shall be in the following order, except as designated by the JTF COS.

(a) Combatant Commander-directed VTCs

(b) CJTF commander-directed VTCs.

(c) Recurring JTF VTCs as required by the JTF battle rhythm

(d) CJTF and component commander requested VTCs (for example, commander to LNOs or other component commander).

(e) JTF HQ staff requested VTCs.

(f) Other requested VTCs.

(2) JWICS VTC. Scheduling is the responsibility of the JTF HQ, Joint Intelligence Center (JIC) director. JWICS VTC use is coordinated through the JWICS System Manager. Prioritization should be the same as for the GENSER VTC. The JTF COS adjudicates scheduling disputes.

e. Visual aids. Visual aids are encouraged for VTCs. However, they must be concise and readable to the viewer. Make every effort to provide advance copies of visual aids to all commands participating in the VTC, before the VTC. Some suggested guidelines for visual aids on GENSER and JWICS VTC are—

(1) Use sentence case (upper and lower case) for text on slides.

(2) Use no smaller than 28-point courier font text for text on slides.

(3) Use pure black and white, when possible, for contrast and ease of reading.

(4) Keep graphics simple.

(5) Mark the classification of visual aids appropriately.

(6) Attempt to display no more than seven lines of text per slide.

(7) Annotate the current date and Zulu time on each briefing.

f. Security. Because of the range of security classifications potentially passed during the VTCs, each location must ensure that personnel with appropriate clearance and access attend the VTCs.

8. Organizational Messaging

a. OSD has directed the closure of AUTODIN, which includes termination of circuits that support AUTODIN and decommissioning the DMS Transition Hubs (DTH). DMS is the Assistant Secretary of Defense for Control, Communications, and Intelligence (ASD 3CI)-designated messaging system for the DOD and supporting agencies.

b. DMS is a flexible, Commercial-off-the-Shelf (COTS)-based application providing multi-media messaging and directory services using the flexible and expandable underlying Defense Information Infrastructure (DII) network and security services. DMS provides message service to all DOD users (to include deployed tactical users); access to and from DOD locations worldwide; and interfaces to other U.S. government agencies, allied forces, and Defense contractors. DMS handles information on all classification levels, compartments, and handling instructions.

c. The DMS program was established as an integrated common-user, organization-to-organization, and individual messaging service. DMS relies on existing and emerging technologies to meet DOD's need for secure, accountable, organization-to-organization, and individual messaging at a reduced cost.

d. DMS provides two grades of enabled service: high and medium grade. The high grade service provides organizational messaging/record traffic to include command and control, combat support, and other functional areas and incompatible, unsecured electronic mail systems. DMS also provides medium grade service, a protected messaging capability for individuals, that leverages the installed base of COTS email products that are administered as standard network services across DOD. The combination of COTS email and DOD PKI security services provides protected individual messaging capability throughout the Services and Defense Agencies.

e. DMS has X.400 based elements of service that provide message redirection/auto forwarding capabilities for after hours notification. Services and agencies are strongly encouraged to develop their own policy and procedures in accordance with U.S. Supplement to ACP 123 and tailored to the organization's operational environment. Requirements for 24 hours per day/7 days per week coverage can be achieved by having messages redirected at the end of the workday to another command or organization that is operational 24 hours per day/7 days per week.

9. Global Broadcast System

The Global Broadcast System (GBS) provides receive-only, high-speed flow of high volume data to units in garrison, deployed, or moving. It supports existing combatant commander requirements by providing the capability to distribute large information products to deployed user platforms. GBS develops and distributes information products according to the CDP to avert saturating deployed forces with information overload. The JTF JIM cell or similar organization is responsible for enforcing the CDP. The following major operational elements of GBS pertinent to IM—

a. Users. Users are deployed warfighters in the combatant commander's AOR. GBS is to be as transparent as possible, while servicing the needs of the users, with required information products.

b. Information Producers. Information producers can be just about anything that produces a product the warfighter wants.

c. Satellite Broadcast Management. Satellite broadcast management executes the GBS broadcast by fulfilling eight basic functions:

(1) Builds a schedule and program guide.

(2) Coordinates information products.

(3) Conducts traffic analysis.

(4) Constructs and transmits the broadcast stream.

(5) Provides for protection of data.

(6) Controls the GBS broadcast technically.

(7) Controls remote enabling/disabling of receive suites.

(8) Establishes and maintains the user profile database.

10. Information Dissemination Management

a. Information Dissemination management (IDM) is a developed and partially fielded COTS/GOTS application suite which provides information sharing capability. IDM combines a tailorable data network search engine with web-based technology enabling users to have access to information customized to their needs based on job function, interests, senior leader information access policies, and/or location. IDM also has rudimentary data routing capability that can select the most effective path to receive information across a data network.

b. IDM has the following capabilities—

(1) Information cataloging. Builds catalogs of information products based on user-designated sources. Users can update these catalogs as required to ensure the most current information products are available.

(2) Information searching. Allows users to search catalogued resources to identify needed information based on user-defined key words or file type. IDM also enables users to search multiple catalogs, including those created by SIPRNET Search Service and IntelLink-S.

(3) Information advertising. Helps information producers match their products with users who need their product, by enabling producers to label information appropriately.

(4) User profile management. Enables users to identify information needed on a recurring basis. This can be information relating to a specific topic or information from certain producers. IDM can retrieve and detect updates to this information, making it available to users.

(5) Senior leader information access policy management. Enables senior leaders to manage information flow within their span of influence. Senior leaders can grant access and the ability to publish specific information to subordinate elements, as well as establish policies to control bandwidth use.

(6) Information delivery. Includes rudimentary data path selection, directory replication, store and forward, and site caching capability that improves efficiency of available bandwidth.

11. Priority of Communication Means

Information and the value of information based on the commander's requirements drive the installation and restoration of communications means. To assist in making this happen, the JTF J6 establishes specific responsibilities for establishing connectivity between the JTF HQ and components. Normally, the higher headquarters is responsible for

establishing all connections to lower headquarters. The JTF should possess redundant means of voice communications, data transfer, and functional specific data systems. The following is a recommended prioritized list of communication means normally found within the JTF. Actual prioritization will be dependent upon CJTF guidance, unique mission requirements, and the situation.

a. UHF TACSAT or HF radio communications network.
   (1) JTF command net.
   (2) Intelligence net.
   (3) Air coordination net.
   (4) Theater missile defense net.
b. Commercial Voice Communications.
c. Defense Switched Network (DSN).
   (1) Commercial secure telephone equipment phones
   (2) Secure telephone unit III (STU-III) phones.
   (3) KY68 tactical lines.
   (4) Defense Red Switch Network (DRSN).
d. Data Transfer.
   (1) SIPRNET/NIPRNET/JWICS.
      (a) Web pages.
      (b) E-mail.
      (c) File transfer protocol (FTP).
   (2) AUTODIN.
   (3) DMS.
   (4) DISA IDM application
   (5) Facsimile.
   (6) TADIL links.
   (7) STU-III file transfer.
e. Functional specific communications.
   (1) SCI intelligence collection-JWICS.
   (2) STU III dial-in.

Chapter V
INFORMATION AND INFORMATION SYSTEM PROTECTION

1. Background

The increasing dependence of societies and military forces on advanced information networks creates new vulnerabilities, as well as opportunities. Potential adversaries could exploit these vulnerabilities through means such as computer network attack and high-power microwave weapons. Advancements in command and control systems contain vulnerabilities that must be mitigated by the CJTF. Mission accomplishment depends on protecting and defending information and information systems from destruction, disruption, and corruption by safeguarding them from intrusion and exploitation. These are critical tenants for mission accomplishment and aid in accomplishing IS, an enabler to full spectrum dominance. Specific duties and responsibilities for information and information system protection within the JTF are listed in chapter II.

2. Threats to Information Systems

In order to ensure information integrity and assurance for the force, the CJTF must have an understanding of the various types of threats to the information systems and the consequences if these threats are not mitigated. Threats against friendly C2 vary by potential adversaries' technical capabilities and motivation. The IMP must anticipate internal and external threats across the full spectrum of conflict. Additionally, sound system configuration along with a proactive network monitoring plan aid in risk mitigation.

a. External threats. Attacks emanating from outside of the network continue to challenge security professionals due to the ethereal complexities of detection. Attack techniques, such as email spoofing or IP hopping, require a significant level of skill for the system administrator to detect and mitigate. Anti-virus software, information assurance vulnerability alerts (IAVAs) and DOD computer emergency response team (DOD-CERT) advisories provide measures to protect against many external attack weapons.

b. Insider threat. Threats emanating from within the joint information infrastructure pose a significant risk to the overall information systems. Individuals with legitimate system access, whether recruited, self-motivated, or through carelessness have entry to information and information systems that are otherwise protected against outside attack. Within the system, a malicious insider may launch a series of computer attacks, which may create spill over effects throughout the entire JTF network.

3. Information Attacks

Note: This section addresses how an opponent may attack friendly IM systems and identifies some basic consideration for the IM organization to consider in defending against such attacks. It is not intended to be a complete IA or CND guide.

a. Computer attacks may employ tailored algorithms or simple methods, with malicious intent. These functions can include activities to disrupt, deny, degrade, alter, or destroy system information. Attacks against information systems can be generally grouped

into four categories— denial of service, social engineering, technical vulnerability exploitation, and sniffing.

(1) Denial of service. Computer network attackers can use a “flood” attack to prevent legitimate users of a network service from using that service. By flooding a targeted system with requests for information, this category prevents legitimate network traffic; attempts to disrupt connections between two machines, thereby preventing access to a service; and attempts to prevent a particular individual from accessing a service.

(2) Social engineering. Computer network attackers can use social engineering techniques to acquire sensitive information or inappropriate access privilege, by building inappropriate trust relationships with network insiders. A computer network attacker may use this technique to gain confidential information (such as organizational charts, phone numbers, procedures or passwords) in order to evaluate the organization's vulnerability to social engineering attacks.

(3) Technical vulnerability exploitation. Technical vulnerability exploitation attempts to conduct attacks which exploit weaknesses in the network infrastructure. It exploits a hardware, firmware, or software weakness or design deficiency to penetrate a system for an unauthorized purpose. Technical vulnerabilities leave an information system open to external as well as internal exploitation.

(4) Sniffing. A computer network attacker may employ a “sniffer”, a computer script designed to monitor network traffic. These programs automatically extract usernames, passwords, credit card account numbers, or other personal information for illicit purposes.

b. Attack Process. A computer network attacker may use one or more information tools (worm, virus, Trojan horse, logic bomb) to exploit a discovered computer system vulnerability. Depending on level of access, the attacker may be free to navigate or control the network. Attacker objectives may be political, destructive, recreational, or for recognition among peers. In order for network administrator personnel to develop policies to protect their networks, they must understand the characteristics of various computer attack processes. As depicted in figure V-1, an attacker uses an information tool to exploit a vulnerability to perform an action on a target in order to achieve an unauthorized result. To be successful, an attacker must find paths that can be connected, perhaps simultaneously or repeatedly.

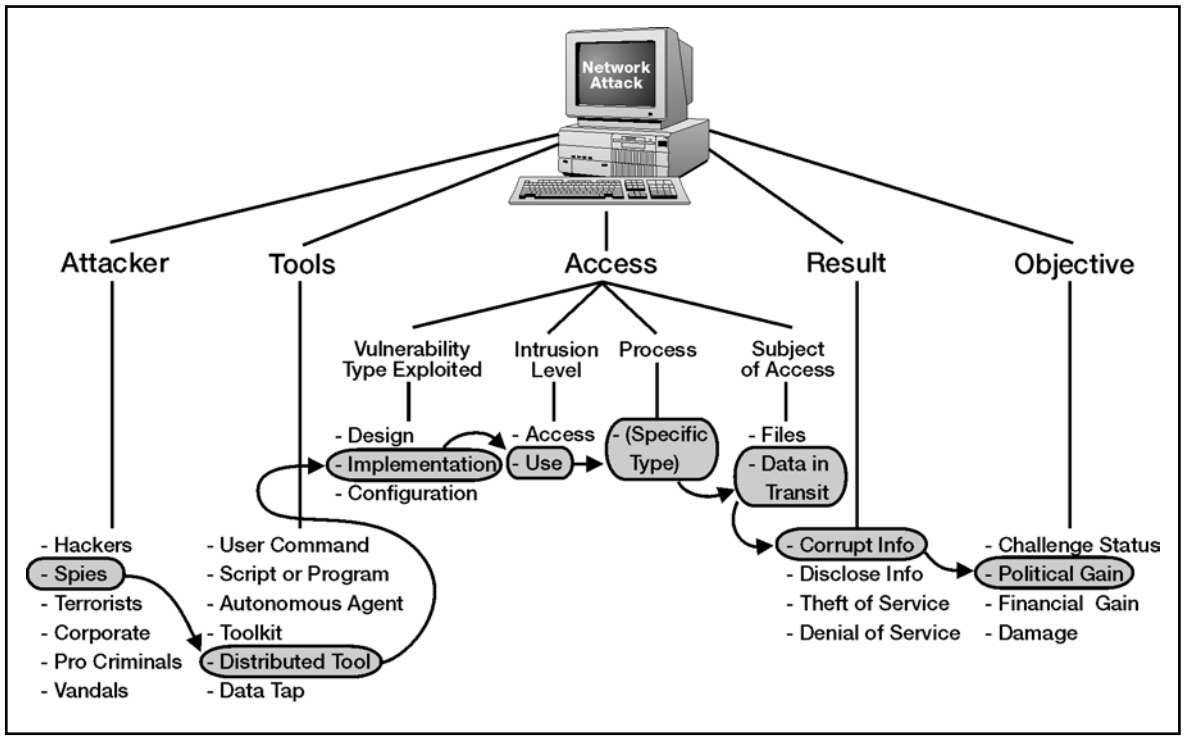


Figure V-1. Basic Taxonomy of Computer and Network Attack

(1) In this instance, JTF J6 staff members must analyze the network from a mission analysis perspective. Mission analysis includes identifying the attacker, determining the objective of the attack, the anticipated result, and the means of achieving the attack. Additionally, this taxonomy allows any given attack to be examined as a process vice a single isolated event.

(2) Denial of service or system degradation from malicious activity may result in a misrepresentation of the battlespace to friendly forces, which leads to lack of situational awareness and understanding. Subsequent effects may also result in the occurrence of false assumptions throughout the mission planning process based on the display of an inaccurate COP. To more effectively leverage friendly capabilities in the battlespace, the CJTF must dedicate adequate resources to protect information and information systems from attack. Regardless of the type of threat (external or internal), the IMP must include in the system configuration a proactive network monitoring plan for joint information systems. Promulgation of a Joint intrusion detection and monitoring plan provides service components and other non-DOD agencies a common operating standard.

4. Information Assurance and Computer Network Defense

a. A key objective of the CJTF may involve operations that may adversely affect an adversary's use of the information spectrum. IA is defined as a set of defensive mechanisms to accomplish this task. The J6 will perform IA duties within the JTF. Chapter II details those IA duties.

b. CND is an operational part of IA. CND relies on a robust IA posture that involves specific actions taken to protect, monitor, analyze, detect, and respond to unauthorized

activity within DOD information systems and computer networks. IA is organized around a defense in depth strategy that integrates the abilities of people, operations and technology to establish multilayered and multidimensional protection.

5. Service Support Organizations

Note: Not all Service CND and IA organizations are listed. Several DOD agencies, such as joint task force for computer network operations (JTF-CNO) and DOD CERT, have established CND support infrastructures to support the operational commander's situational awareness.

a. JTF-CNO. JTF-CNO acts as the DOD agent for CND and computer network attack (CNA). The JTF-CNO is located in Washington, DC, with the DISA as it's supporting agency. This allows the JTF-CNO to be collocated with DISA's Global Operations and Security Center and to leverage DISA's existing global presence, its network operational view, intrusion analysis, and core technical capabilities with the unified commands and the law enforcement community.

b. DOD CERT. The DOD CERT works in conjunction with JTF-CNO, regional network operations and security centers, regional computer emergency response teams (RCERTs), law enforcement agencies, intelligence agencies, Service CERTs, and the Joint Staff to provide CND technical analysis expertise through monitoring and protecting DII systems and networks. DOD CERT functions are—

(1) Collect information about new vulnerabilities.

(2) Release IAVA, when the vulnerability is most severe and corrective action is of the highest priority.

(3) Release information assurance vulnerability bulletin (IAVB), when the vulnerability does not pose an immediate threat to DOD systems, but is significant enough that non-compliance with the corrective action could escalate the threat.

(4) Release a technical advisory, when the vulnerability exists, but is categorized as low risk.

(5) Protect, defend, and restore the integrity and availability of the essential elements and applications of the DII.

(6) Responsible for global intrusion detection, vulnerability analysis and management, and the investigation of incidents.

(7) The virus support team performs analysis to determine whether a suspicious event was caused by malicious code, and if so, provides appropriate guidance to the customer.

c. Service support infrastructure. Most Service agencies are organized along the protect; monitor, analyze and detect; and respond paradigm as illustrated in figure V-2. For brevity purposes, not all specific Service organizations and their roles are listed.

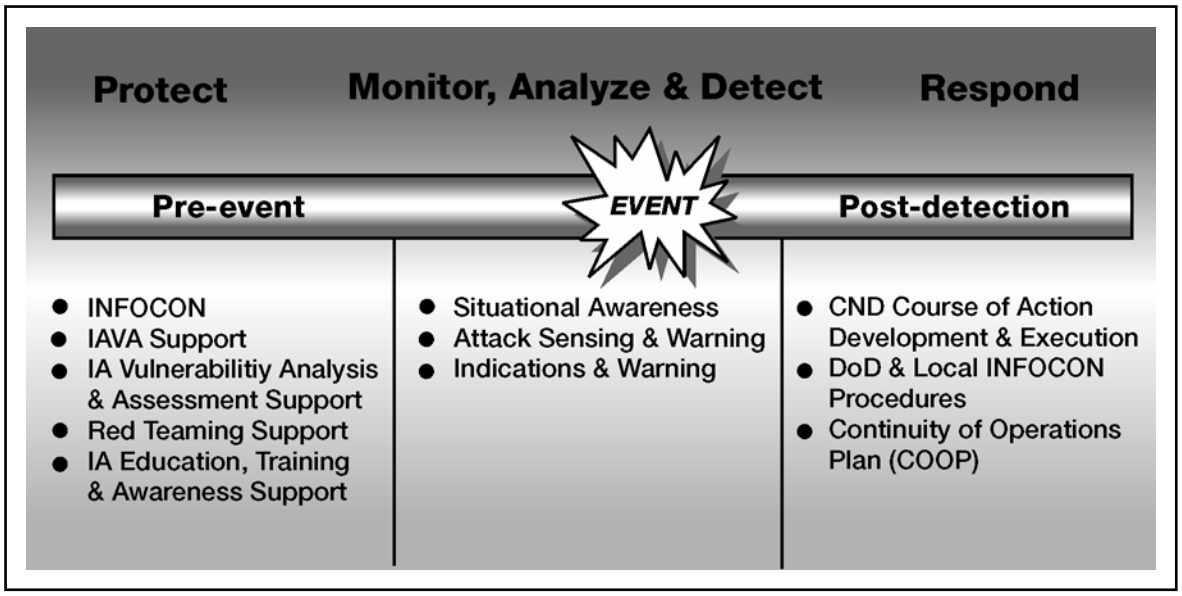


Figure V-2. Typical CND Support Infrastructure

6. Protect Measures

CND Protect includes the management of DOD's information operations conditions (INFOCONs) system and deliberate actions taken to modify an information system or computer network configuration or assurance posture in response to a CND alert or threat information. It also includes support for activities such as the IAVA system; vulnerability analysis and assessments; and IA and CND education, training, and awareness.

a. Information operations conditions. The DOD INFOCON system establishes a uniform and operational approach for posturing and defending against malicious activity targeted against DOD information systems and networks, and for achieving a common level of information security. The INFOCON system is characterized by a set of defensive postures consisting of directed measures implemented uniformly across the DOD. Effective 1 October 2002, the SECDEF delegated to USSTRATCOM the authority to declare DOD INFOCON levels.

b. INFOCON levels and guidance. The DOD INFOCON system is comprised of five progressive levels: Normal, Alpha, Bravo, Charlie, and Delta. These five levels characterize a range of network defensive measures that support information operations at all levels of conflict, from peacetime to wartime. Specific measures and actions are outlined in CJCSM 6510.01A.

(1) INFOCON Normal. CND operations are routine and there exists normal readiness of DOD information systems and networks. There is little risk to ongoing military operations; information networks are operational. Operational impact of degradation or loss of information and information systems is low.

(2) INFOCON Alpha. Increased intelligence watch and strengthened security measures of DOD information systems and networks. Attributes are—

(a) Indications and warning (I&W) indicate general threat.

(b) Regional events occurring which affect US interests and involve potential adversaries with suspected or known CNA capability.

(c) A military operation, contingency or exercise is planned or is ongoing which requires increased security of information systems.

(d) Information system probes, scans, or other activities detected indicating a pattern of surveillance.

(3) INFOCON Bravo. A further increase in CND force readiness above that required for normal readiness. Attributes are—

(a) Indications and warning (I&W) indicate targeting of specific system, location, unit or operation.

(b) A major military operation or contingency is planned or ongoing.

(c) Significant level of network probes, scans or activities detected indicating a pattern of concentrated reconnaissance.

(d) Network penetration or denial of service attempted with no impact to DOD operations.

(4) INFOCON Charlie. A further increase in CND force readiness, but less than maximum CND force readiness. Intelligence attack assessment(s) indicate a limited attack. Attributes are—

(a) Information system attack(s) detected with limited impact to DOD operations.

(b) Minimal success, successfully counteracted.

(c) Little or no data or systems compromised.

(d) Unit able to accomplish mission readiness.

(5) INFOCON Delta. Maximum CND force readiness. Attributes are—

(a) Successful information system attack(s) detected which impact DOD operations.

(b) Widespread incidents that undermine ability to function effectively.

(c) Significant risk of mission failure.

7. Joint Task Force Computer Network Defense Operations

The CJTF is presented with the challenge of making operational decisions based upon information; obviously, the commander's perception of the characteristics of that information is involved in that process. At the tactical unit level, the commander's administrative reach is commensurate with his/her operational reach. Previous knowledge of the IA status and understanding of the Service CND hierarchy normally results in strong confidence (or doubt) about the information at hand. The CJTF operates at a higher echelon of command, on an ad-hoc basis, and with units of other Services (each using different operational concepts), making this same confidence more elusive. Higher levels of command rely on reports, both formal and informal, from subordinates to gauge the capability and readiness to accomplish assigned missions. Parent Services normally define the nominal capability for specific units or weapons systems, leaving the readiness

reporting to the tactical units. The CND posture of the JTF is heavily dependent upon the CND service providers in the constituent units' parent services (see figure V-3).

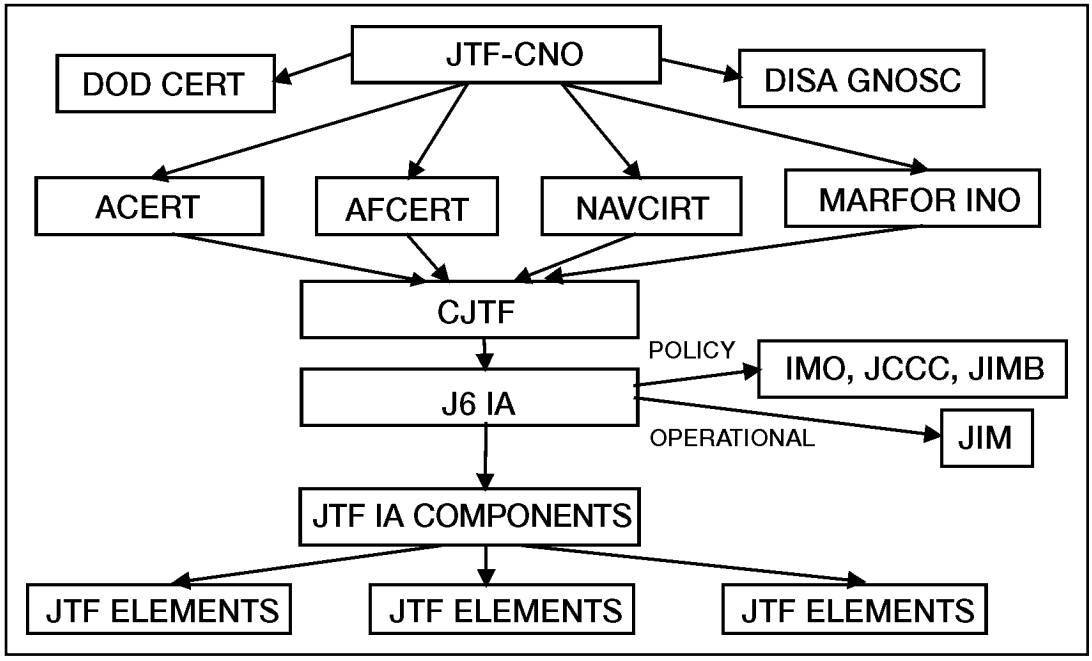


Figure V-3. Proposed JTF IA Structure

8. Information Security

The mission, intelligence and course of action are all information specific to the situation. This information requires a CJTF decision on criticality and level of protection. Unit movements, logistic support, intelligence requirements and other information are developed based upon these in a growing pyramid of potential indicators. IP networks provide unparalleled data transport capacity and flexibility, but are not the only means of information transport. Voice and fax communications over switched circuits, tactical radio circuits and tactical data links are all other forms of communication between units. The operational needs of the CJTF may determine whether a transient network outage is a minor or major problem. Assessment of time required for these indicators to reach the enemy and the pace of friendly operations are key factors in the CJTF decision. The following methods should be considered for the protection of information related to JTF operations:

a. Classify information properly.

b. Protect passwords.

c. Use cryptographic tools such as virtual private networks to provide a level of protection for information traveling through non-cryptographically protected networks.

d. Do not use work-around communications solutions.

9. Techniques for Effective INFOCON Management

With familiarity of INFOCON policy directives, JTF system administrative (SYSAD) personnel must develop management techniques that allow swift transition to varying levels of INFOCON, without jeopardizing their warfighting capability. This section provides planning aspects used in effective management of information systems for supporting INFOCON.

a. Identify Mission Critical, Mission Support, and Administrative Information Systems and Networks. Effective INFOCON management commences with SYSAD personnel identifying critical information nodes within their infrastructure. The types of IA protective measures, techniques and procedures needed for a system shall be determined on both information security and mission criticality. CJCSI 6510.01C sets policy for the assignment of all DOD information systems to a mission category (mission critical, mission support, or administrative). Generally, higher levels of security are required for higher levels of system critically and information sensitivity. Also, this method provides JTF components with a capability to develop preparatory measures, response actions, and restoration activities to ensure continuation of mission-essential functions. Continuity of information systems and networks are an inherent part of DODD 3020.26.

b. Develop User Groups. The IMP must include a prioritized information systems positions/users list. This list will identify users who require system access to perform mission essential duties on unclassified and classified networks. The list shall not be solely based on rank or pay grade criteria. Those personnel who are key information processors should be placed into an appropriate user group to support mission accomplishment. The IMO shall design user groups to limit access as much as feasible, and continue all operations with due regard to OPSEC and INFOSEC. The following provides an example of user group categories during periods of increased INFOCON—

(1) User Group One. Provides limited access during a short notice event. Access limited to: key staff members, commander, planners, key staff officers, etc.

(2) User Group Two. Intended to maintain an increased INFOCON policy while allowing key personnel the access necessary to conduct detailed planning and critical operations. Access includes—user group one, key staff personnel, department heads and senior division officers, watch officers, and all mission essential personnel authorized by the CJTF.

(3) User Group Three. Provides greater access to unclassified information systems and includes user groups one, two, and personnel E-7 and above.

(4) User Group Four. The least restrictive, allowing normal access to all information systems for all authorized users.

(5) For Windows NT applications, user groups can be established in the Microsoft exchange server or in the primary domain controller, thus allowing a simplified implementation when INFOCON levels are changed.

(6) For Windows 2000 applications, active directory, dynamic domain name service, and group policy provide techniques for user group management.

(7) UNIX (i.e. SUN, SOLARIS, HP-UX, Linux) supports both password and group files on the local system as well as the Network Information Service (NIS). NIS supports the concept of a “netgroup”, and allows certain netgroups of users to have access to a

particular machine. SUN also offers a more secure NIS+ variant. UNIX offers methods to control access to files by classifying access in three ways—Owner (or single user), UserGroup, and Everyone. Access control lists (ACLs) must be utilized to restrict access of information to several groups or select individuals of a specific group. ACLs provide precise control over a number of users and groups accessing files and directories.

c. Develop an INFOCON quick reference matrix of critical systems. As with any other operational posture, INFOCON poses a unique challenge with managing information systems. A matrix of critical information systems along with their status during varying INFOCON levels provides a standard approach to protecting systems within the JTF organization. Additionally, this approach helps to control outgoing information (for example, via computers, phones, facsimile, radio/telephone circuits, etc.) to support INFOSEC, COMSEC, force protection condition, and OPSEC planning.

(1) COOP. Risk to operations is the primary consideration when establishing an INFOCON. The intent of the INFOCON system is to provide a predictive tool such that decisions to raise the INFOCON level are made to mitigate risk and ensure continuity of operations. Within the deliberate planning process, planners examine operational factors of information systems that support higher echelon objectives. These factors include the operational status of information networks, the risk to the commander's ability to process and disseminate information, and the actual or potential operational impact of degraded information networks. JTF planners should attempt to measure the adversarial threat through an operational impact assessment.

(2) The operational impact assessment provides a comprehensive procedure to identify all mission critical information systems prior to malicious activity, and a means to examine the technical impact after malicious activity has been detected. Details of the assessment will provide a metric by which the operational commander can declare regional INFOCON, or justify non-compliance of certain INFOCON directives. Upon completion of the operational impact assessment, the IMO can develop a COOP based upon actual mission requirements and information system capabilities. As an integral part of the IMP, the COOP may include the following—

(a) List of critical information systems related to their respective mission.

(b) Authorized users list, distinguished by tier groups.

(c) Local INFOCON procedures.

(d) INFOCON quick reference matrix of critical systems.

(e) Operational impact assessment of mission.

(f) Reporting instructions.

10. Impact Assessment Process

a. Assessing the impact of malicious activity or computer network attack on the ability to conduct military operations is key to conducting damage assessment, prioritizing response actions, and assisting in identifying possible adversaries. Figures V-4 and V-5 provide examples of operational impact assessment tools.

b. PRIOR TO ANY MALICIOUS ACTIVITY. Following are the initial steps that should be taken prior to the possibility of any malicious activity—

(1) Identify all critical information systems.

(2) For each critical information system, identify all resident critical applications and databases.

(3) Determine which military functions are supported by each application/database: command and control; intelligence, surveillance, and reconnaissance; movement and maneuver; logistics; fires and protection.

c. AFTER MALICIOUS ACTIVITY HAS BEEN DETECTED. After malicious activity has been detected, the following steps should be followed—

(1) Identify all critical information systems targeted.

(2) List missions or operations the unit is currently supporting, or projected to support in the near future, that may be affected by this activity.

(3) For each information system targeted, determine the technical impact, i.e., to what degree are confidentiality, integrity, availability, authentication, and non-repudiation affected? What critical applications and databases are impacted?

(4) For the technical impacts identified, estimate the time and resources required to restore functionality. Identify any interim workarounds.

(5) Determine how the technical impact of the malicious activity affects the unit's ability to execute its mission.

(6) Determine how the impact on the unit's ability to function affects support to current/projected operations. If no specific operations are ongoing or projected, make a determination of how general capability/readiness is affected.

DATE/TIME (Z) _____
INFOCON LEVEL _____
EMCON LEVEL _____
CURRENT OPERATIONS _____

		MISSION/OPERATION FUNCTIONS (√) INDICATES MILITARY FUNCTIONS SUPPORTED BY EACH APPLICATION/DATABASE												
A.CRITICAL INFORMATION SYSTEMS	B. ASSOCIATED APPLICATION/ DATABASE	AT/FP	CSAR	CTTG	FONOPS	HA/DR	MIO	NEO	PEACE KEEPING	SEAD	STRIKES AND RAIDS	TRAP	LOGISTICS	OTHER
SAMPLE														

EVALUATE IMPACT TO MISSION/OPERATION IF LOSS OF CRITICAL SYSTEM

CRITICAL SYSTEM	OPERATIONAL IMPACT TO MISSION/OPERATION IF LOSS OF CRITICAL SYSTEM How does the technical impact of the malicious activity affect the unit's ability to execute its mission? How does the impact on the unit's ability to function affect support to current/projected operations? If no specific operations are ongoing or projected, how is general capability/readiness affected?

Figure V-4. INFOCON Operational Impact Assessment (before malicious activity)

DATE/TIME (Z) _____
INFOCON LEVEL _____
EMCON LEVEL _____
CURRENT OPERATIONS _____

			IMPACT TO MISSION/OPERATION FUNCTIONS (√) INDICATES MILITARY FUNCTIONS SUPPORTED BY EACH APPLICATION/DATABASE												
A.CRITICAL INFORMATION SYSTEMS TARGETED	B.TECHNICAL IMPACT TO INFORMATION SYSTEM	C. ETA FOR SYSTEM RESTORATION	AT/FP	CSAR	CTTG	FONOPS	HA/DR	MIO	NEO	PEACE KEEPING	SEAD	STRIKES AND RAIDS	TRAP	LOGISTICS	OTHER
SAMPLE															
EVALUATE IMPACT TO MISSION/OPERATION DUE TO LOSS OF CRITICAL SYSTEM															
CRITICAL SYSTEM	OPERATIONAL IMPACT TO MISSION/OPERATION How does the technical impact of the malicious activity affect the unit's ability to execute its mission? How does the impact on the unit's ability to function affect support to current/projected operations? If no specific operations are ongoing or projected, how is general capability/readiness affected?														

Figure V-5. INFOCON Operational Impact Assessment (after malicious activity)

Appendix A
NON – DOD INFORMATION MANAGEMENT INTEGRATION GUIDELINES/CHECKLIST

1. General

The mission assigned a JTF will require not only the execution of responsibilities involving two or more military departments but increasingly, the support of all types of U.S. governmental and nongovernmental organizations (NGOs). The CJTF has at least two responsibilities usually associated with those of combatant commanders—the requirement for unified action in the CJTF's JOA and the necessity to interface with U.S. government and host nation agencies. The JTF HQ serves as the operational focal point for interagency coordination.

a. Non-DOD agency operations can be grouped into two general categories—domestic and foreign operations.

b. Identify and appoint a liaison officer for each non-DOD organization. For additional information concerning liaison operations, see ALSA's JTF Liaison Handbook (FM 5-01.12, MCRP 5-1B, NTTP 5-02, AFTTP (i) 3-2.21).

c. Identify policy/framework for information exchange requirements between DOD and non-DOD agencies (need to know; access).

d. Identify technical communications link parameters.

e. Identify information security exchange parameters.

f. Establish joint interagency coordination group (JIACG)/civil-military operations center (CMOC).

g. Incorporate JIACG/CMOC/non-DOD agency battle rhythm.

h. Incorporate non-DOD information requirements into IMP and CCIR.

i. Ensure JIACG know and understand media/PAO guidelines/guidance.

j. Incorporate non-DOD/JIACG/CMOC annexes into overall JTF plans and orders.

k. Define command relationships with non-DOD/JIACG/CMOC.

l. Identify to CJTF new requirement for forces, personnel, equipment, etc to support non-DOD/JIACG/CMOC requirements.

m. Conduct mission analysis in coordination with JTF staff.

n. Identify and define endstate of planned and ongoing operations.

o. Develop and recommend appropriate courses of actions to support the JTF.

2. Liaison Checklist

The following checklist can be used as a guide to aid in the flow of information between the JTF and external organization:

a. Telecommunications systems compatibilities and requirements.

(1) Radio channels, call signs, and frequencies—see your frequency manager.

(2) Network connectivity and bandwidth requirements.

(3) VTC interfaces and bridges.

(4) Media feed.

(5) Phone links.

(6) Phone books.

(7) Data transmission protocols, for example,—AppleTalk, TCP/IP, Novell Internetwork package exchange (IPX).

b. Information systems compatibility.

(1) IA tools.

(2) Desktop operating systems.

(3) Email bridges and gateways.

(4) Office application.

(5) Network operating system.

(6) Firewall.

(7) Router protocols and polices.

(8) Digital rules of protocols—file interface standards.

(9) Web site adjustments.

(10) Main frame.

(11) Operational requirements.

(12) Synchronize daily rhythms and operation times.

(13) Organization structure and chain of command.

(14) Action officers/LNOs.

(15) Reporting procedures.

(16) Utility requirements.

(17) Power.

(18) Air conditioning.

(19) Infrastructure.

(20) Classified access requirements.

Appendix B
RECORDS MANAGEMENT

1. Introduction

Records, regardless of physical form or characteristics, must be managed to comply with the Federal laws governing records management. The National Archives and Records Administration (NARA) issued regulations in 1995 that include the requirement to manage e-mail messages as records when created in the conduct of government business. Because the requirement to manage electronic records exists, the JTF must use either Joint Interoperability Test Command (JITC) certified electronic record keeping software or manual procedures to manage their records. The purpose of this section is to assist records managers (RMs) and records custodians (RCs) in managing electronic records and e-mail records using manual procedures.

a. Background. User requirements for data storage on the network continue to grow rapidly. Despite repeated upgrades in storage techniques and capacity, the demand quickly reaches and exceeds capacity. Excessive volumes of stored data can adversely impact overall system performance and increase restoration time in the event of certain network system failures. Due to personnel turbulence and other factors, our current system of user-based data administration is not effective. Analysis by systems administrators indicates that much of the data currently stored may be obsolete or redundant. As a result, specific data management procedures are required.

b. Electronic Recordkeeping. The Office of the Assistant Secretary of Defense (Command, Control, Intelligence, and Communications [C3I]), Information Technology, developed standards for electronic record keeping (ERK) applications. The DISA (Joint Interoperability Test Command (JITC) obtained final approval for DODD 5015.2-STD in December 1997. COTS records management software applications are being tested for compliance with federal requirements. Those meeting DOD standards are listed in a registry of certified electronic records management (ERM) software at: http://lyris@jitc.fhu.disa.mil/recmgt/register.htm. All DOD agencies will be required to purchase ERM software applications from those listed in the registry.

c. Interim Solution. Managing electronic records ensures integrity throughout the record's life cycle. The interim solution to manage control of electronic records is a methodology using files and directories that coincide with paper records management. RMs and RCs will comply with these procedures and assist action officers in organizing their electronic records.

d. Benefits.

(1) Locate information quickly and easily.

(2) Reduce paper record holdings.

(3) Re-use of information.

(4) Reduce space required to stage paper records.

(5) Transition more easily to an electronic record keeping application.

(6) Assist in administering command history programs.

2. Responsibilities

a. JTF RM.

(1) Administer the combatant command records management program for all command records, including Top Secret-sensitive compartmented information (TS-SCI), special access program, and focal point records to facilitate collection of all relevant documentation.

(2) Provide life cycle management of combatant command and headquarters staff records, recorded on any media (this includes e-mail), to include identification, maintenance, storage, retirement, and destruction.

(3) Submit annual records reports, through the Joint Secretariat to the chairman of the Joint Chiefs of Staff.

(4) Provide for records collection and retention in mobilization planning and crisis action procedures, to include command operations center records.

(5) Ensure that records management appendixes or annexes are included in appropriate operations plans, operations orders, and concept plans. These annexes will specify how records will be collected and retained.

(6) Ensure the adequacy of the command's records management program, from a historical perspective, and facilitate liaison between the historian and the command records manager—to ensure that key documents, including electronic records, are reviewed, organized, and secured.

(7) Ensure command personnel are trained to meet records management requirements— to include appropriate security, policy, and legal procedures.

(8) Ensure regular records management assistance visit inspections are made to staff directorates and all subordinate activities/agencies.

(9) Assist RMs in the implementation and administration of ERM.

(10) Maintain a list, with e-mail addresses, of assigned directorate RMs and alternates. Provide J6 help desk personnel with new lists as updates are made.

b. Records managers.

(1) The RMs may appoint RCs, as required, to maintain below directorate-level office file disposition and maintenance plans.

(2) Train and grant permissions for the file disposition and maintenance plans to appointed RCs.

(3) Enforce the file retention limits for assigned network drives. Monitor appointed RCs to ensure file retention limits are enforced.

(4) Approve requests for outside offices to access directorate network drives.

(5) Report changes of assigned Directorate RM and alternate to the JIMB Secretariat and command RM.

(6) Manage the two-letter organization drive for their respective directorate.

(7) Implement ERM.

(8) Manage the overall maintenance of the directorate's shared drive. RMs will have "Full Control" rights to electronic files within their directorate. RMs can in turn, delegate "Read/Write/Assign Permissions" controls to their RCs.

(9) Assist records custodians in understanding ERM principles/applications.

(10) Ensure records are properly being cut-off, purged, disposed of, transferred, and filed.

(11) Archive records to compact disk (CD) on or before the 1st of March for calendar year records.

(12) Archive records to CD on or before 1st of Nov (for fiscal year records).

Note: The CD Software has a 64-character limit on the subject line.

(13) Maintain the CD until the retention period is met.

c. Record custodians.

(1) Enforce file retention limits on assigned network drive(s).

(2) Interface with office network users to ensure familiarity with electronic file plans, data storage procedures, retention limits, JTF records management policies and procedures and appropriate security and legal policy and procedures. Provide one-on-one training for all new office personnel.

(3) Manage division level files disposition and maintenance plans on designated drives.

(4) Accomplish end of year closeout for fiscal year and calendar year records by transferring records to the inactive files area and/or destroying those records no longer needed. Apply basic records management principles to manage electronic records according to disposition instructions.

(5) Assign appropriate rights to users of e-file areas.

(6) Assist action officers with understanding electronic filing requirements.

d. Action officers (AO).

(1) Determine which records are official PERMANENT records that need to be maintained.

(2) Work with RMs and RCs to file official records in the proper electronic file, or e-mail record to records custodian for proper filing.

e. JCCC.

(1) Manage compliance of network drive storage and audit log back up procedures for all assigned JTF networks.

(2) Periodically review all network drives to ensure users and RMs properly manage them. Send notices as required.

(3) Backup and restore the network drive data. Differential backups include only data that has been modified since the last full backup. Full backups include the entire data

set. Storage includes on- and off-site locations to ensure recovery in the event one of the locations is destroyed (see table B-1).

Table B-1. Example Data Backup Schedule

Occurrence	*Data*	*Backup Type*	*Day(s) Performed*	*On-site/Off-site Storage Duration*
Daily	User, common, E-mail	Differential	Sunday-Thursday	3 months
Weekly	User, common, E-mail and system	Full	Full	3 months
Quarterly	User and Common	Full	Last Sunday of quarter	1 year
Annual	User and Common	Copy of current year's quarterly backups	December 31	3 years

(4) Create and modify user accounts to make the required network drives available to the user upon logon.

(5) Grant required data permissions to users and RMs for their respective network drives.

(6) Load authorized applications on JTF personal computers (PCs) and servers. JCCC production engineering personnel are the only persons authorized to load applications on any JTF connected computer. This is a security and virus protection requirement. All other applications are unauthorized and J6 personnel are required to delete them upon discovery.

f. Files maintenance and disposition plan.

(1) Creating the electronic file plan.

(a) RMs and RCs ensure the directorate file plan is approved and current. All file plans are approved by JTF RM and chopped through the directorate RM.

(b) RMs and RCs annotate in the file plan where the official (permanent) electronic or hardcopy record is filed.

(2) Implementing the electronic file plan.

(a) Establish electronic file plan by creating folders or directories and subdirectories on the K: drive that reflects the items from the authorized file plan. (It is not necessary to create a directory for each item on the file plan; just the items to be filed electronically). Names of the files, folders, directories, and subdirectories should be limited in character length and abbreviated when possible. This will prevent file paths exceeding any character restriction imposed by the operating system.

(b) Figure B-1 provides an example of an electronic file plan. Each directorate will only have access to their particular directorate's files.

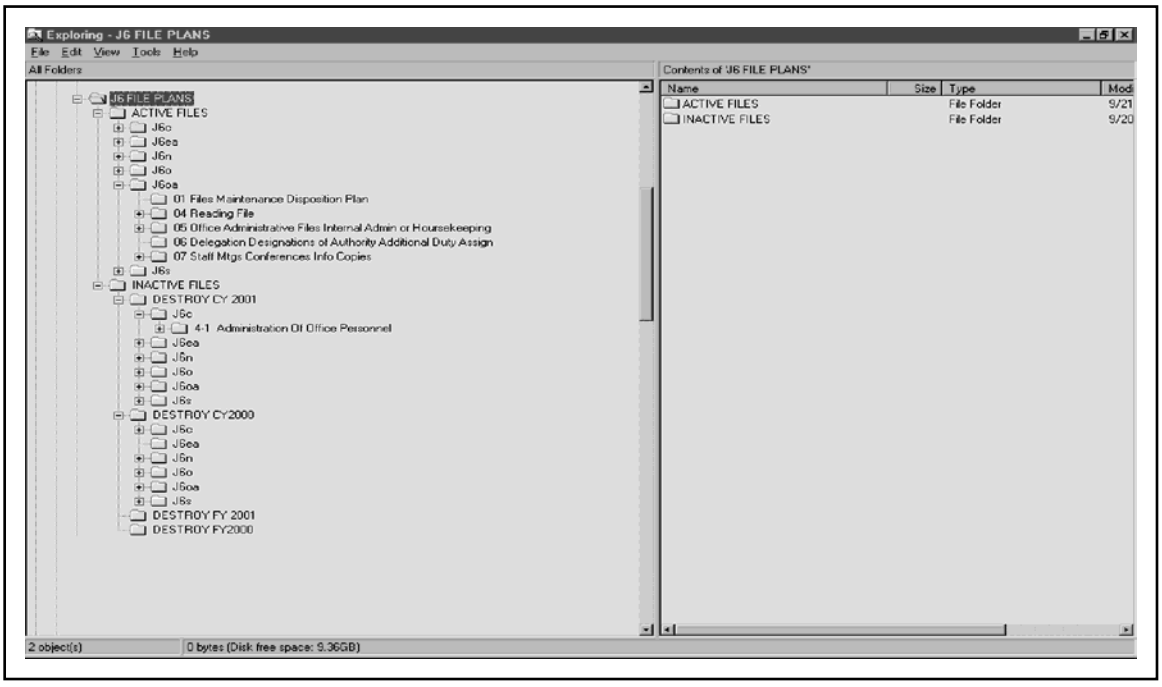


Figure B-1. Example Electronic File Plan

(3) "Active Files".

(a) The active folder will contain subdirectories for every office of record.

(b) Prior to filing the official PERMANENT record in the electronic file plan, save record as a "READ ONLY" file.

(4) "Inactive Files".

(a) The inactive folder will contain subdirectories for every office of record. Subdivide each inactive directory by the year material is to be destroyed.

(b) Establish an INACTIVE directory for each record series requiring transfer to inactive status at the end of the fiscal or calendar year.

(5) Records maintenance. Maintain records electronically when feasible. Maintain paper copies if a signature is required for legal or financial purposes.

(6) File disposition. Disposition of electronic records should coincide with the disposition instructions listed for the respective items. The interim solution provides for electronic files management in the same way paper files are managed until an automated system is established. If a signed paper copy is required for legal or financial purposes, file the paper copy.

(a) Filing e-mail records. The requirement exists to maintain and dispose of e-mail messages the same way as other electronic records. Most e-mail records are temporary records and should be reviewed and destroyed annually. However, if policy is being made via e-mail, the e-mail becomes a permanent command record and should be treated the same as other electronic and hardcopy permanent files.

- Ensure the e-mail record includes transmission data that identifies the sender and the recipient(s) and the date/time the message was sent and/or received.

- Retain the e-mail distribution list for the same retention period required for the e-mail message.

- Retain a record of names of e-mail addressees when the e-mail system uses codes or aliases to identify senders or recipients.

- File attachments to the e-mail as part of the electronic record.

- Do not file "information only" e-mail. Only file e-mail requiring action or e-mail needed for adequate and complete documentation.

- Ensure federal records sent or received on e-mail systems outside organizational control are preserved. Ensure reasonable steps are taken to capture available transmission and receipt data needed by the agency for record-keeping purposes.

- When the e-mail record is retained in a record-keeping system, delete the e-mail message from the e-mail system.

(b) Freedom of Information Act (FOIA) for records and e-mail. Some records are exempt from release if the release would cause identifiable harm. The following categories of information are normally exempt from routine disclosure and must be protected from unintentional or unauthorized disclosure: classified information; internal personnel rules or practices; information specifically exempted from disclosure by another statute; confidential commercial information; inter- or intra-agency record that is in deliberation or is predecisional in nature; information whose disclosure would constitute an invasion of privacy; records or information compiled for law enforcement purposes. Do not send information normally exempt under FOIA across the Internet without an appropriate level of protection to prevent unintentional or unauthorized disclosure.

(c) Protection of e-mail addresses. To reduce the risk of attack on e-mail systems, do not indiscriminately release e-mail addresses. Lists of individual and organizational e-mail addresses are exempt from disclosure under the FOIA as internal information.

(d) The requirement exists to provide retrieval, use and print capability for the life cycle of the record. If system upgrades will result in loss of these capabilities, paper copies of records will be printed and filed.

Appendix C
INFORMATION MANAGEMENT PLAN CHECKLIST

This checklist is provided as a quick reference for IM personnel to ensure their IMPs cover all necessary information. Examples of different IMPs are also provided below as references, however, users should tailor their IMP to the situation and needs of their JTF.

Example warfighting IMP: CJTF180 (Operation Enduring Freedom) KIMP at: http://www.acc2langley.af.smil.mil/alsa/cjtf180kimp.doc

Example future-oriented IMP: US JFCOM Millennium Challenge 2002 (MC02) KIMP at: https://lad.dtic.mil/alsa/mc02kimp.doc

Example consequence management-oriented IMP: NORTHCOM JTF-Civil Support IMP at: https://lad.dtic.mil/alsa/jtfcsimp.zip

1. Introduction

a. Purpose.

b. Scope.

2. JTF IM Organization

a. JTF—

(1) CJTF.

(2) Chief of Staff.

(3) IMO.

(4) JIMB.

(5) JIM.

(6) Others, as required.

b. JTF IM roles and responsibilities—

(1) JTF IM Organization.

(2) JTF Components.

(3) Allies and Coalition Partners.

c. Higher headquarters and other organizations—

(1) Higher headquarters.

(2) Other organizations – (NGO/PVOs/Non-DOD U.S. government organizations).

3. Commander's Dissemination Policy

a. Critical information elements.

b. Relative priorities of information flows.

c. Relative priorities of information users depending on—

(1) User.

(2) Organization.

(3) Mission.

(4) Information type (survival information, admin information, operational information, intelligence information).

d. Information release policies—

(1) Public affairs guidance.

(2) Release of real time operational information to subordinate units, allies, and coalition partners.

(3) Release of real time intelligence information to subordinate units, allies, and coalition partners.

e. Information priority policies—

(1) CCIR.

(2) Communication network architecture.

(3) Information operations goals and objectives.

(4) Identification of routine information products.

f. Limit access to specific information by content, source, type or location.

g. Releasability of information transfer due to security or classification policy.

4. Information Requirements and General Procedures

a. CCIR—

(1) FFIR.

(2) PIR.

b. RFIs.

c. COP management.

d. Collection management.

e. Records management—

(1) Records managers responsibilities.

(2) Records custodians responsibilities.

(3) Action officers responsibilities.

(4) Information technology services branch responsibilities.

(5) Files maintenance and disposition plan.

(6) Records maintenance and disposition policies.

(7) Records collection.

f. Reports.

5. Digital Rules of Protocol

a. Virtual meeting rooms facilitator.

b. Audio practices—standard military radio\telephone procedures should be employed.

c. Text chat practices.

d. Session/meeting closure.

e. Collaboration tools file cabinets.

f. Whiteboard.

g. Virtual conference center/auditorium collaboration.

h. Ad hoc meetings via chat.

i. Document file naming convention.

j. Briefing slide show file production and management.

k. File management.

l. Calendar operations.

6. Battle Rhythm

(Applicable to each organization pursuant to their procedures.)

7. Information Assurance/Computer Network Defense

a. Info priority matrix of critical mission systems.

b. Information confidence convention (ICC)—

(1) Info source assurance and reliability.

(2) Info currency.

(3) Info content and completeness.

(4) Use of the ICC.

c. Computer network defense—

(1) Joint intrusion detection and monitoring plan.

(2) Information assurance vulnerabilities assessment (IAVA).

(3) Information operations condition actions.

(4) Operational impact assessment.

(5) Continuity of operations plan.

8. Information System Tools and Procedures

a. Tactical data systems.

b. Collaborative tools.

c. Voice communications.

d. LAN/WAN management.

e. Data management.

f. Electronic messaging—

(1) Organizational messaging.

(2) E-mail.

(3) Chat.

9. System Recovery Procedures

(Applicable to each organization pursuant to their operating system.)

Appendix D
DIGITAL RULES OF PROTOCOL

1. Overview

The following are a set of recommended procedures to follow to ensure proper use and promote proper etiquette when working with collaboration tools and other digital information systems within a JTF. These procedures were taken from the 2002 JFCOM Millennium Challenge (MC02) exercise knowledge and information management plan (KIMP). The entire MC02 KIMP is available at the ALSA website at: https://lad.dtic.mil/alsa/mc02kimp.doc. These procedures represent future IM concepts and technologies and are provided to assist IM planners and organizations in developing digital rules of protocol and to see potential IM practices in the future.

Note: Some organizations use the terms digital rules of engagement or business rules. This publication uses the term DROP to avoid any possible confusion with established joint force rules of engagement (ROE).

2. Virtual Meeting Rooms

This is collaboration among individuals; each may have an active voice in the proceedings.

a. Leadership and preparatory actions.

(1) The leader appoints a deputy to assist in administration (post agenda, archive session chat, keep time, and take notes/minutes). These duties may be delegated to more than one member of the meeting.

(2) Participants log in 5 minutes prior to start time, check in (voice and chat) with the deputy. If a member attends as a generic user, such as "Planner 22," then that user should include a more specific identification either in the chat conversation or on the bulletin board.

(3) A facilitator, while not always available, enhances the collaboration and shortens the meeting.

b. Audio practices.

(1) Standard military radio telephone procedures should be employed.

(a) Identify yourself prior to speaking.

(b) Keep statements short and relevant, and use "Break" for a pause in longer statements.

(c) Speak slowly.

(d) End transmission with "Over" or "Out" as appropriate.

(e) Push the talk button and hold prior to talking. Be sure that your microphone button is on and off as appropriate. A "stuck microphone" will disrupt the audio for everyone.

(2) Be aware of your voice volume – in the limited work spaces normally associated with contingencies, you may prevent the person sitting next to you, who is in another collaborative meeting, from hearing through his headset.

(3) Respect others who are speaking.

(4) Limit use of private audio, as many collaboration systems do not support multiple simultaneous audio conversations well. Use text chat for sidebar discussion, or check out of a meeting to talk, and then return.

c. Text chat practices.

(1) Keep statements short.

(2) Use private chat for sidebar conversations.

(3) Remember everyone in a room (and those that join after) can review all prior conversations which occurred within the chat room.

(4) Important open room chat logs should be copied and pasted into a Word or WordPad document, and stored with meeting minutes in the file cabinet associated with the meeting place.

d. Session/meeting closure.

(1) Participants should notify the meeting group, via chat, prior to departure from session, who will cover issues of their concern.

(2) Meeting recorder will review action item responsibilities (this may be best done by text chat or any other text tool.)

(3) Specify location of meeting notes/minutes posting and the location of any slide shows used by presenters.

(4) Specify time/location of next meeting.

e. File cabinet. Collaboration tools file cabinets will be used for temporary storage of documents under construction and those to be used in upcoming collaborative sessions. Some tools may have no document history or version control. When document development is completed and final approval is received the document will be transferred to the appropriate location. Meeting minutes must be kept. Slide shows should be maintained for version control.

f. Whiteboard. The room whiteboard function allows the occupants of a virtual room to view and annotate the whiteboard at the same time. Users can interactively manipulate, annotate, and save the whiteboard contents. The whiteboard can import multiple file types. Multiple images can be imported and displayed on the whiteboard simultaneously.

(1) The contents of the whiteboard may be saved, as an individual file and redisplayed as desired. The number of saved whiteboard files is limited only by the collaboration tool server capacity.

(2) Whiteboard images and annotations can be saved as a file in the room file cabinet, or downloaded to a user's workstation.

(3) Do not load images or make annotations to the whiteboard until instructed to do so by the team leader or a designated representative. This will prevent accidental erasure of whiteboard contents.

(a) Use only your assigned color to make annotations to the whiteboard. Suggested assigned colors are listed in Table D-1.

Table D-1. Whiteboard Annotations

Service Components
Combatant Command HQ - BLACK
ARFOR - GREEN
MARFOR - RED
NAVFOR - BLUE
AFFOR - CYAN
Theater SOC - ORANGE
Functional Components
Combatant Command HQ -BLACK
JTF HQ - GRAY
JFLCC - GREEN
JFMCC - BLUE
JFACC - CYAN
JSOTF - ORANGE

(b) Before clearing annotations or images from the whiteboard, notify all users in the room and provide them with an opportunity to save the whiteboard.

(c) Upon completion of the meeting or session, the assigned deputy will erase the whiteboard display to prevent inadvertent disclosure of sensitive information.

3. Virtual Conference Center/Auditorium

This is collaboration between a presenter or a panel of presenters, and a mostly passive audience of up to several hundred. Meeting procedures listed above apply in this venue, to the extent possible.

a. Presenters.

(1) Primary – Primary briefer for the session will upload the slides to be presented into the auditorium file cabinet. The first slide will show the file address in the auditorium file cabinet.

(2) Alternate/questions – The alternate briefer is responsible for answering posted questions (this allows the primary briefer to continue), and announces where the briefing and minutes will be posted in the JTF web portal.

(3) Systems Administrator – Provides technical assistance as required.

(4) Note taker – Keeps track of taskings, recommendations, and questions (copies questions posted into the minutes at conclusion of the session and posts the minutes to the JTF web portal as directed).

b. Audience members log in at least 10 minutes prior to start time, check in (voice and chat) with deputy. If a member attends as a generic sign on, such as “Planner 22,” then a specific identification should be immediately placed in the chat.

(1) Choose a seat in a row to facilitate chat in an interest group.

(2) Change rows to coordinate with other groups.

(3) Questions encouraged by chat - focused on meeting issues.

(4) Private chats may be used to increase collaboration.

4. Ad Hoc Meetings via Chat

The active users function provides a listing of all users logged into the virtual collaboration environment and current room location. Users may contact one another without leaving their respective rooms.

a. Invite – Invites addressee to join you in your room.

b. Join – Transports you to the room of the person selected.

c. Send Note – Sends a text message.

d. Chat – Opens a private chat window.

e. E-mail – sends an e-mail through MS Outlook.

5. Document File Naming Convention

Consistent document naming is essential to proper workings of the collaboration tool. All files (documents, presentations, spreadsheets, etc.) will conform to the following naming convention.

a. Arabic numerals only (no Roman numerals).

b. No date-time group (DTG) or version number EXCEPT for documents of historic reference, that will remain unchanged and may have legal or other significance. In these cases, a DTG is appropriate. (for example: the DTG of a brief that the CJTF has received and approved should be marked at the time of approval.)

c. No spaces, fill spaces with underscore.

d. Separation of parent document and specific document: hyphen.

e. Example: The Information Operations Matrix for ETO 1B is named: ETO_1B-IO_Matrix (Parent Document: ETO_1B)(Specific Document: IO_MATRIX).

6. Briefing Slide Show File Production and Management

Every effort will be made to reduce, if not eliminate, formal briefing presentations. Any briefings prepared should conform to the rules and format outlined below so as to reduce transmission bandwidth and system storage requirements. Format slides are located below.

a. Basic text slides - remove logos - pictures only when required.

b. Keep them short (<15 is ideal) - if longer brief is required, break it into sections with question/clarification breaks.

c. Text Arial - title - 36 (32 if two lines), subtitle - 28, 1st level - 28, 2nd level - 24, 3rd level - 20, Footers – 14.

d. Text emphasis - bold, underline & italics - limit use of colors – use only when required and only colors that stand out well.

e. Text spacing (Tool Bar, Format, Line Spacing) minimums - lines 0.90, returns 0.25.

f. Footer - lower right - slide #, lower left - DTG of briefing version, bottom center – point of contact info and JTF portal posting location.

g. If graphics are necessary, the image concerned must be grouped and then saved as a .gif, or .jpg files, and then placed on a blank PowerPoint slide.

7. File Management

Consistent handling of digital files is critical to building the JTF digital information library. Organization of the files in a way that allows easy access and the removal of incorrect information or outdated knowledge from the digital library is important. These are the individual responsibilities:

a. Preservation of files.

b. Place all gained information regarding a JTF into the appropriate database.

(1) Save only links to files, program executes and websites on your desktop.

(2) Save nothing on the C drive of any PC.

(3) Save personally gained information and researched information on your H drive until such time as you deem it "trusted.

(4) Save trusted information in a common file server, unless it is specifically applicable to a special interest user community.

(5) Save files and create enhanced file folders under the appropriate area file, such as Plans, IS, IM or Operations. Because of permissions, you may not be able to conduct file management outside your own organizational area.

c. Organization of the files in a way that allows easy access.

(1) Name your files and folders in a way that others will obviously recognize the content.

(2) Familiarize yourself with the taxonomy of the filing system, or consult your staff section IM coordinator to ensure appropriate file or folder location.

(3) Collaborate with your co-workers to build consistency of thought in the organization of the files.

(4) During the process of saving or editing documents, pay careful attention to the file properties. When entering file properties, place yourself in the users' shoes and ask: "How will my customer think to search this information?" Market your information!

(5) Inspect the web pages that display your information links frequently to ensure that they provide the expected document. In our open environment of information sharing, the links to web pages are easily broken. Notify your staff information manager, or if unavailable any information manager of bad web links.

(6) Do not change the file name of a document after it has been published to the user community.

d. The removal of incorrect information.

(1) Inspect files and folders that you have some ownership in periodically to ensure veracity of content. Decision: Leave it there, archive it, or take it out of the database.

(2) The decision to archive is taken in the case that the information is not current, but is correct or useful as historical reference. With concurrence of your staff information manager, move these items to the designated archive file. Ensure the context of the file name is maintained, creating new folders in the archive as necessary. This information is still available to the search engines.

(3) To remove files, DO NOT DELETE! Only information managers may delete files. To take files out of the information library, move them to the junk folder designated by your staff IM. Notify your staff IM when you do this.

8. Calendar Operations

a. Microsoft Outlook calendar functions will be used to conduct a number of operations in scheduling and management of JTF collaborations.

(1) The JTF Common Use Calendar will be maintained for the purpose of coordinating all JTF staff collaborations.

(2) The IS, Plans, and Operations groups may maintain their own calendars for the specific purpose of their own groups' management. When these calendars are used, they will be linked to the JTF calendar, such that the JTF calendar shows all entries.

(3) All Boards, Centers, and Cells will scheduled on the calendar, specifically inviting the required and optional members with the meeting reminder enabled. In addition, the invitations will have the location and the fall back procedure/location in case of system failure. The agenda of the will be posted in the text area of the invitation. The recurring meeting feature is recommended for standing meetings. If this is used, the meeting owner should review the invitation list and agenda daily.

b. The JTF Calendars. The central planning calendar for the JTF is "JTF "Named Operation" Calendar," which is the only centralized calendar in the JTF organization. The staff groups may, at their option, operate a group calendar for their own convenience, but these will all feed the centralized JTF calendar.

c. JTF "Named Operation" Calendar. Joint Task Force – "Named Operation" will use a consolidated calendar for tracking all JTF Battle Rhythm events. All JTF personnel have read access to the calendar but author permissions are currently limited to the personnel listed in table D-2.

Table D-2. Authorized Calendar Users	
Command Group	JTFSJS JTFKMOCG
Information Superiority Group	JTFISCoord JTFDepISCoord JTFCurrentSitOff SJFHQISConceptMntr SJFHQKMOIS
Operations Group	SJFHQLandOps2 SJFHQKMOOps
Information Management Group	JTFKMOLead SJFHQKMOLead
Plans Group	JTFAIRPLNS1 SJFHQARMYPLANNER SJFHQKMOPLANS

9. Additional Guidelines

a. Don't use e-mail for sensitive or emotionally charged issues. Personnel, personal, or work-related issues that have certain sensitivities are best handled with either a face-to-face meeting or telephone call.

b. Don't use e-mail to disparage others. E-mail is an effective medium for conveying information; however, it is totally inappropriate to use e-mail to disparage or "flame" others.

c. Be aware: no e-mail is private. Keep in mind any e-mail sent to others becomes part of the public record. Don't send e-mail to individuals unless you wouldn't mind that e-mail being seen by either the CJTF or public media.

d. Blind courtesy copy (bcc). Limit use of the bcc. There is no assurance that the bcc recipient won't forward it to unintended audiences.

e. Limit non-mission essential e-mail. Jokes, stories, and inessential .avi or .jpg files may temporarily improve morale; however, they tend to clutter the local communication infrastructure. Please limit use of e-mail to only mission-essential traffic.

References

Joint

DODD 3020.26, *Continuity of Operations Policy and Planning (COOP)*, 26 May 1995.

DODD 5015.2-STD, *Design Criteria Standard for Electronic Records Management Software Applications*, 19 June 2002.

DODD 5200.1-R, *Information Security Program*, January 1997.

DODD 8000.1, *Management of DOD Information Resources w/change 1*, 20 March 2002.

DODD 8500.1, *Information Assurance (IA)*, 24 October 2002.

DODD 8910.1, *Management and Control of Information Requirements*, 11 June 1993.

JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*, 9 June 1998.

JP 6-02,*Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations*, 30 May 1995.

JP 6-02, *Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems*, 1 October 1996.

CJCSI 5760.01, *Records Management Policy for the Joint Staff and Combatant Commands*, 10 March 2003.

CJCSM 5760.01 *Volume 1 & 2, The Joint Staff and CINC Records Management Manual*, 10 March 2003.

CJCSM 3122.03, *JOPES Volume II, Planning Formats and Guidance, Enclosure C,* 1 June 1996.

CJCSM 6510.01C, *Information Assurance and Computer Network Defense*, May 2001.

Army

FM 3-0, *Operations*, 14 June 01 (FM 100-5).

Future Publications:

FM 3-13, Information Operations Doctrine and TTTP (FM 100-6).

FM 5-0, *Army Planning and Orders Preparation* (FM 101-5).

FM 6-0, *Mission Command: Command and Control of Army Forces* (FM 100-34).

Marine Corps

MCDP 6, *Command and Control*, 4 October 1996.

Navy

Naval Doctrine Publication 6, *Naval Command and Control*, 19 May 1995.

Air Force

Air Force Manual 37-104, *Information Management*, 1 June 1995.

Air Force Doctrine Document 1, *Basic Doctrine*, 1 September 1997.

Air Force Doctrine Document 2, *Organization and Employment of Air Power*, 17 February 2000.

Air Force Doctrine Document 2-5, *Information Operations*, 04 January 2002.

Air Force Doctrine Document 2-8, *Command and Control*, 16 February 2001.

Air Force Operational Tactics, Techniques, and Procedures 2-3.2, *Air and Space Operations Center*, October 2002.

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

A

ABN	airborne
ACL	access control list
ACP	airspace control plan
AELT	aeromedical evacuation liaison team
AFDC	Air Force Doctrine Center
AFFOR	Air Force forces (a Service component of a joint force)
AFI	Air Force instruction
AIS	automated information system
ALSA	Air Land Sea Application Center
AMHS	Automated Message Handling System
AO	action officer
AOR	area of responsibility
ARFOR	Army forces (a Service component of a joint force)
ATO	air tasking order
AUTODIN	Automatic Digital Network

B

BBS	bulletin board system
bcc	blind courtesy copy
BDA	bomb or battle damage assessment

C

C2	command and control
C3I	command, control, intelligence, and communications
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
CA	civil affairs
CAN	computer network attack
CAT	crisis action team
CCIR	commander's critical information requirement
C-Day	unnamed day on which a deployment operations begins
CDP	commander's dissemination plan
CDR	commander
COMLANTFLT	commander, Atlantic fleet

CERT	computer emergency response team
CINC	commander in chief
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CJTF	commander, joint task force
CMOC	civil-military operations center
CND	computer network defense
COA	course of action
COGARD	Coast Guard
COLISEUM	community online intelligence system for end users and managers
COMM	commercial
COMSAT	communications satellite
COMSEC	communications security
CONOPS	concept of operations
COOP	continuity of operations plan
COP	Global Command and Control System common operational picture
COPB	Global Command and Control System common operational picture board
COPC	Global Command and Control System common operational picture cell
COPM	Global Command and Control System common operational picture manager
COS	chief of staff
CTP	common tactical picture
CVBG	carrier battle group
CWAN	coalition wide area network

D

DAA	designated approving authority
DCJTF	deputy commander, joint task force
DCTS	Defense Collaborative Tool Suite
D-Day	unnamed day on which operations commence or scheduled to commence
DET	detachment
DII	defense information infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISUM	daily intelligence summary
DMS	defense message system
DNVT	digital nonsecure voice terminal
DOD	Department of Defense

DODD	Department of Defense directive
DROP	digital rules of protocol
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DSVT	digital subscriber voice terminal
DTG	date-time group
DTH	defense message system (DMS) transition hubs
DVS-G	digital video services—global

E

E-7	enlisted pay grade level 7
EEFI	essential elements of friendly information
EEI	essential elements of information
E-mail	electronic mail
EPW	enemy prisoner of war
ERK	electronic record keeping
EWO	electronic warfare officer
EXORD	execute order

F

Fac	facility
FAX	facsimile
FDESC	force description
FFIR	friendly force information requirements
FOB	forward operations base
FOIA	freedom of information act
FP	force protection
FPO	fleet post office
FRAG	fragment
FRAGO	fragmentary order
FTP	file transfer protocol

G

GBS	Global Broadcast System
GCCS	Global Command and Control System
GENSER	general service (message)

H

HF	high frequency

HQ	headquarters
HQ AFCENT	Headquarters, Allied Forces, Central Europe
HQUSAFE	Headquarters, United States Air Forces in Europe
Hrs	hours
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocols

I

I&W	indications and warnings
IA	information assurance
IAVA	information assurance vulnerability alert
IVAB	information assurance vulnerability bulletin
ICC	information confidence convention
IDM	information dissemination management
IM	information management
IMB	information management board
IMC	information management coordinator (staff)
IMO	information management officer
IMP	information management plan
info	information
INFOCON	information operations condition
INFOSEC	information security
Intel	intelligence
INTSUM	intelligence summary
IO	information operations
IP	Internet protocol
IPX	Internetwork package exchange
IRC	Internet relay chat
IS	information superiority
ISB	intermediate staging base
ISR	Intelligence, surveillance, and reconnaissance
ISSM	information systems security manager
ISSO	information systems security officer
IT	information technology
IW	information warfare

J

J1	Manpower and Personnel Directorate of a joint staff
J2	Intelligence Directorate of a joint staff
J3	Operations Directorate of a joint staff

J4	Logistics Directorate of a joint staff
J5	Plans Directorate of a joint staff
J6	Command, Control, Communication, and Computer Systems Directorate of a joint staff
JAC	joint operations center/joint intelligence support element assessment cell
JASC	joint action steering committee
JCCC	joint communications control center
JCMOTF	joint civil-military operations task force
JCS	Joint Chiefs of Staff
JDISS	joint deployable intelligence support system
JFACC	joint force air component commander
JFC	joint force commander
JFCOM	joint force command
JFLCC	joint force land component commander
JFMCC	joint force maritime component commander
JIACG	joint interagency area coordination group
JIB	joint information bureau
JIC	joint intelligence center
JICO	joint interface control officer
JIM	joint information management (cell)
JIMB	joint information management board
JISE	joint intelligence support element
JITC	joint interoperability test command
JMRO	Joint Medical Regulating Office
JOA	joint operations area
JOC	joint operations center
JOPES	Joint Operation Planning and Execution System
JP	joint publication
JPG	joint planning group
JPOTF	joint psychological operations task force
JSOTF	joint special operations task force
JTA	joint terminal architecture
JTCB	joint targeting coordination board
JTF	joint task force
JTF-CNO	joint task force for computer network operations
JULLS	Joint Universal Lessons Learned System
JWICS	Joint Worldwide Intelligence Communications System

K

KIMP	knowledge and information management plan

L

LAN	local area network
LNO	liaison officer
LOGSITREP	logistic situation report
LTIOV	latest time information of value

M

MACOM	major Army command
MARFOR	Marine Corps forces (a Service component of a joint force)
MCCDC	Marine Corps Combat Development Command
MCDP	Marine Corps doctrinal publication
MCO2	2002 joint force command (JFCOM) millennium challenge
MCPDS	Marine Corps publication distribution system
med	medical
MESL	mission essential subsystems list
METOC	meteorological and oceanographic
MEU	Marine expeditionary unit
MEU/ARG	Marine expeditionary unit/amphibious ready group
mic	microphone
MLS	multilevel security
MOA	memorandum of agreement
MSAL	master suspense action log
MSC	major subordinate command
MSEL	master scenario events list
MSG	message
MTTP	multi-Service tactics, techniques, and procedures

N

NAVFOR	Navy forces (a Service component of a joint force)
NAVSOP	Naval standard operating procedure
NAVSTA	naval station
NBC	nuclear, biological, and chemical
NEO	noncombatant evacuation operation
NGO	nongovernmental organization
NIMA	National Imagery and Mapping Agency
NIPRNET	Nonsecure Internet Protocol Router Network

NIS	network information system
NLT	not later than
NSO	network security officer
NWDC	Navy warfare development command

O

OCR	office of collateral responsibility
OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPR	office of primary responsibility
OPS	operations
OPSEC	operations security

P

PAO	public affairs office/officer
PIR	priority intelligence requirements
PLA	plain language address
PM	provost marshal
POC	point of contact
POL	petroleum, oils, and lubricants
PSYOP	psychological operations

R

RC	records custodian
RECERT	regional computer emergency response team
RECCE	reconnaissance
RFA	request for assistance
RFI	request for information
RMA	records management application
ROE	rules of engagement
RR	railroad

S

SAM	surface-to-air missile
SAR	search and rescue
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SECDEF	Secretary of Defense
SIMLM	single integrated medical logistics management

SIPRNET	SECRET Internet Protocol Router Network
SITREP	situation report
SJA	Staff Judge Advocate
SOF	special operations forces
SOP	standing operating procedures
SOTA	signals intelligence (SIGINT) operational tasking authority
SSO	special security officer
ST&E	security test and evaluation
STU-III	secure telephone unit III
SYSAD	system administration brand
SYSCON	system control

T

TACON	tactical control
TADIL	tactical digital information line
TASO	terminal area security officer
TCP/IP	transmission control protocol/Internet protocol
TMD	theater missile defense
TPFDD	time-phased force and deployment data
TRADOC	United States Army Training and Doctrine Command
TRAP	Tactical receive equipment and related applications
TS	top secret
TS-SCI	top secret—sensitive compartmented information
TSCO	top secret control officer
TTP	tactics, techniques, and procedures

U

UHF TACSAT	ultrahigh frequency tactical satellite
UNIX	A multiuser, multitasking operating system originally developed by AT&T (for example: SUN, SOLARIS, HP-UX, Linux).
US	United States
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USMTF	United States message text format
USN	United States Navy
USPACOM	United States Space Command
USSOUTHCOM	United States Southern Command
USTRANSCOM	United States Transportation Command
USSTRATCOM	United States Strategic Command

V

VTC	video teleconference/teleconferencing

W

w	with
WARNORD	warning order
WMD	weapons of mass destruction
WWW	World Wide Web

Z

ZULU	time zone indicator for Universal Time

PART II – TERMS AND DEFINITIONS

battle rhythm - See daily operations cycle.

common operational picture (COP) - A single, identical display of relevant information shared by more than one command. A common operational picture facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called COP (JP1-02). Army definition is: an operational picture tailored to the user's requirements, based on common data and information shared by more than one command (FM 3-0)

common tactical picture (CTP) - The CTP is derived from the CTD and other sources and refers to the current depiction of the battlespace for a single operation within a combatant commander's AOR including current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peacetime through crisis and war. The CTP includes force location, real time and non-real-time sensor information, and amplifying information such as METOC, SORTS, and JOPES. (CJCSI 3151.01)

commander's critical information requirements (CCIR) - A comprehensive list of information requirements identified by the commander as being critical in facilitating timely information management and the decisionmaking process that affect successful mission accomplishment. The two key subcomponents are critical friendly force information and priority intelligence requirements, also called CCIR. (JP 1-02)

daily operations cycle - The schedule of significant recurring events of the JTF HQ staff. The JTF chief of staff normally establishes this to deconflict the JTF staff schedule. This schedule allows JTF staff members to anticipate when information is required and backward plan to ensure inputs are available when needed, also called "battle rhythm".

emoticons - A sideways facial glyph formed by keyboard symbols, which used in e-mails to indicate an emotion or attitude, as to indicate intended humor (:-)).

information filter - Assessing the value of information and culling out that which is not pertinent or important

information flow - Term used to describe movement of information.

information fusion - The logical blending and integration of information from multiple sources into an accurate, concise, and complete summary

information management (IM) - The provision of quality information to the right person at the right time in a usable form to facilitate understanding and decisionmaking.

IM board (IMB) - The focal point for coordinating information management within a JTF HQ. Chaired by the JTF IMO, this board operates under the supervision of the JTF chief of staff, or other appropriate staff directorate, as best meets the JTF requirements. This board should be composed of the senior IMO from each staff section, component, and supporting agency. The board actively resolves all cross-functional information management issues, convening on an as required basis. Also called IMB.

information operations (IO) - Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (JP 1-02)

information security - The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. (JP 1-02)

JOC/JISE Assessment Cell (JAC) - An optional cell to maintain operational awareness of the battlespace through continuous fusion and assessment of all-important friendly and enemy information.

request for information (RFI) - 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. 2. The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. Also called RFI. (JP 1-02)

INDEX

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

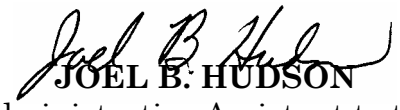
FM 6-02.85 (FM 101-4)
MCRP 3-40.2A
NTTP 3-13.1.16
AFTTP(I) 3-2.22

10 SEPTEMBER 2003

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:



JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: Distribute in accordance with the initial distribution number IDN 115770, requirements for FM 6-02.85.

By Order of the Secretary of the Air Force:

DAVID F. MacGHEE, JR.
Major General, USAF
Commander
Headquarters Air Force Doctrine Center

Air Force Distribution: F