USMC

MCTP 3-30B
(Formerly MCWP 3-40.2)

Information Management

US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 147 000030 00

USMC

CD&I (C 116)

2 May 2016

ERRATUM

to

MCWP 3-40.2

INFORMATION MANAGEMENT

1. Change all instances of MCWP 3-40.2, *Information Management*, to MCTP 3-30B, *Information Management.*

2. Change PCN 143 000094 00 to PCN 147 000030 00.

3. File this transmittal sheet in the front of this publication.

PCN 147 000030 80

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes through the Universal Need Statement (UNS) process. The UNS submission process is delineated in Marine Corps Order 3900.15_, *Marine Corps Expeditionary Force Development System*, which can be obtained from the on-line Marine Corps Publications Electronic Library:

http://www.marines.mil/News/Publications/ELECTRONICLIBRARY.aspx.

The UNS recommendation should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Addition/deletion of text
  - Proposed new text

Additional copies: If this publication is not an electronic only distribution, a printed copy may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status*. An electronic copy may be obtained from the United States Marine Corps Doctrine web page:

https://www.doctrine.usmc.mil.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
WASHINGTON, D.C. 20380-1775

18 June 2014

FOREWORD

Marine Corps Warfighting Publication (MCWP) 3-40.2, *Information Management*, builds on the doctrinal foundation established in Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*. Since the original publication of MCDP 6, technology improvements have led to more effective command and control capabilities; yet, overly complex information processes have left warfighters with new challenges. Further, while Joint doctrine provides broad overarching guidance for information management (IM), it gives few practical solutions for the technological challenges that warfighters face.

This publication provides an overview and definition of the concept of information management, presents examples and guidance for IM strategies, suggests best practices, details IM responsibilities, and presents organizational constructs for IM planning and execution. Its focus is at the tactical and operational levels and it refers to relevant theater strategic issues as necessary. This publication is organized around the pillars of command and control—information, people, and the command and control support structure—because information management is a key command and control enabler.

As stated in MCDP 6, "there is no substitute for effective command and control" and the leadership responsibilities that come with staff organization and collaboration. This publication serves as the authoritative reference for IM concepts and introduces knowledge management, highlighting its relationship to command and control. The intended audience is commanders, staffs, IM officers, communication officers, and information technology users.

This publication supersedes MCWP 3-40.2, *Information Management*, which is dated 24 January 2002.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

K. J. GLUECK, JR.
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration

Publication Control Number: 143 000094 00

This Page Intentionally Left Blank

TABLE OF CONTENTS

Chapter 4. Information Management Processes and Procedures

Appendices

Glossary

References and Related Publications

CHAPTER 1
INTRODUCTION TO INFORMATION MANAGEMENT

Foundation

Information management by itself is an enabler of command and control rather than a discrete element of it. The pillars of command and control are people; information; and the command and control (C2) support structure, which includes organizations, procedures, equipment, facilities, training, education, and doctrine. Figure 1-1 depicts the information flow of these elements.

Marine Corps Doctrinal Publication (MCDP) 6, *Command and Control*, refers to information management; however, it provides no specific definition for it and focuses instead on the definition and elements of command and control conceptually. This publication, however, focuses on information management (IM) processes and procedures as a C2 enabler, integrating people and technology with efficient processes for improved commander situational awareness and focusing information for decisions at the operational and tactical levels of war.

Information Environment

As emphasized in MCDP 6, warfighters function in a physical and political environment of uncertainty: combat is by its very nature chaotic, disruptive, and unpredictable. Data collected and processed in such an environment can often be inaccurate or misleading and the resulting information may be too late, unimportant, or irrelevant to be useful. A commander who innately understands the correlation between quality information and the ability to make timely, effective decisions is able to build a reliable understanding of the challenges he faces. This relationship between the concepts of quality information and understanding remains unchanged from the past, but advances in computing and communication technologies have exponentially increased the volume of available data.

The demands of war have always led to an effort to combine new technology with tactics, techniques, and procedures (TTP) to build warfighting

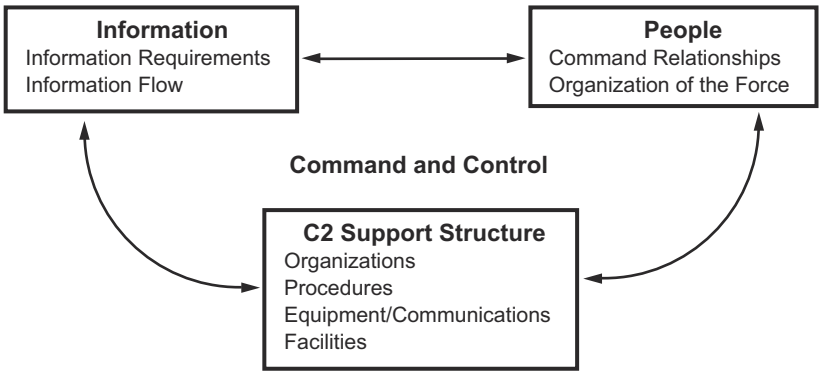


Figure 1-1. Elements of Command and Control.

capabilities. The desire is that the resultant capability of combining technology, procedure, and human intervention will provide tactical advantage against adversary vulnerabilities, allowing the defeat of enemy strengths to achieve the desired end state. As a lever provides the force to move the heaviest weight, so information is the "lever" that increases the commander's speed of action, allowing him to capitalize on an information advantage and influence the environment or the adversary.

The operational environment faced by leaders today is significantly different from even the most recent past. It can be characterized by smaller, technology-enabled military forces; agile unconventional adversaries; interorganizational and multinational relationships; and a fast moving global information forum. These and other factors contribute to an increasingly dynamic, complex, and interrelated arena in which Marines must operate, which requires adjustments in information TTP to provide necessary operational agility. Today's operational environment is heavily influenced by the technology revolution and the explosive growth of technology systems.

Technology Revolution

The technology revolution and resulting abundance of new C2 systems and applications have exponentially increased the complexity and amount of data that must be viewed, sorted, collated, disseminated, and managed by military forces. Operational level headquarters can no longer rely solely on the electronic mail (e-mail) inbox to understand, visualize, plan, and direct operations. Organizations that do not adapt to technological advances may become overwhelmed or distracted, losing the ability to maintain relevant situational awareness and/or make timely and informed decisions. Communications and network-centric capabilities are covered in greater depth in the Marine Corps Warfighting Publication 3-40 series.

Leaders make decisions based upon their personal understanding of a situation; such an understanding develops through information assimilation and refines through the lens of personal experience, intuition, and judgment. Historically, commanders achieved this understanding or situational awareness by personally viewing and visiting the battlefield; however, as the size, tempo, and complexity of the modern battlefield expanded, this approach became untenable.

To compensate for modern warfare realities, commanders and their staffs gain battlefield perspective from situation maps, text documents (e.g., messages, reports, status boards), and voice reports. The situation map and text information, combined with the commander's experience, intuitive reasoning, judgment, and personal contact with frontline units, enables the commander to attain a level of understanding necessary to make informed decisions. Contending with the complexity characterized by conflict in the 21st century, warfighters need not only integrated systems, but also structured policy and guidance. Such direction should be combined with procedures that collect, process, and safeguard data and thereby facilitate efficient information assimilation, sharing, and collaboration. The aggregate of today's technology, procedures, people, and policy must provide shared situational awareness and decision support across a distributed network in dynamic and chaotic arenas.

Information Management Pillars

Conceptually, information management provides the right information to the right people at the right time for situational awareness or decisionmaking. It consists of three mutually supporting pillars: people, technology, and process (see fig. 1-2). People (customers and data processors) are the ultimate users of information; they provide expectation, policy, and guidance for the end product. Technology (hardware and software) is the physical network and systems used by people to collect and process data. Process (procedures and

policy) is the implementation of best practices that integrate the three pillars, provide efficiency, and eliminate duplication for effective information flow according to the operational requirement. Aligning the three pillars focuses the collaboration or C2 capability (technology) for its intended effect, and helps implement any necessary alternative solutions for integration shortfalls.

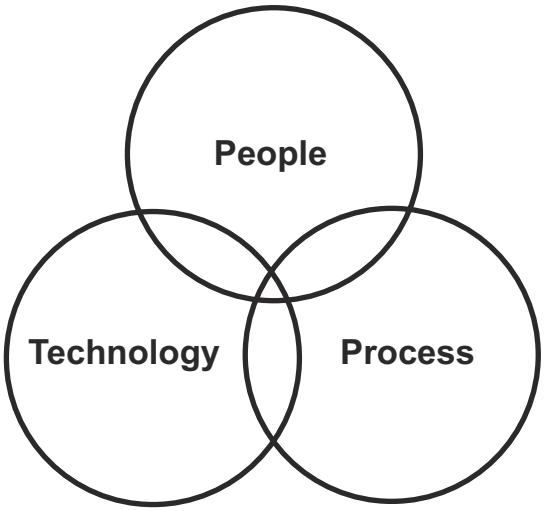


Figure 1-2. Pillars of Information Management.

Warfighter Impact

Poor or nonexistent information management has consequences that burden the warfighter, impact information flow, and disrupt operational efficiencies. If any of the key elements are missing or poorly managed, the commander will achieve no benefit from information management. Poor information management tends to incorrectly focus on the seams and gaps of technology systems, integration shortfalls, or lack of operator training; whereas, proper information management focuses on improving processes. Poor information management burdens the warfighter with duplicative solutions, which fatigues users and frustrates battle system efficiencies.

Information management and knowledge management enable operational functions and organizational learning to improve mission performance across the Marine Corps. Marine Corps Order 5400.52, *Department of the Navy Deputy Chief Information Officer Marine Corps Roles and Responsibilities*, recognizes the inherent relationship of information management and knowledge management (discussed further in chap. 2) as a function of the command element. Therefore, the Deputy Commandant for Combat Development and Integration is the identified advocate.

Advancing technology has changed the way the Marines Corps leverages its C2 systems to influence the operational environment. Timely, quality information provides required situational awareness to commanders and adds value to the decisionmaking process—both of which impact mission accomplishment.

The management of the flow of this information and access to it are critical. Information management helps commanders focus their people, technology, and processes most effectively to meet challenges and leverage fleeting opportunities.

Information is a valuable commodity, bringing with it an added dimension of both situational context and technical complexity. It is an asset that must be effectively managed by aligning people, technology, and process to allow warfighters to compete successfully.

This Page Intentionally Left Blank

CHAPTER 2
INFORMATION MANAGEMENT DEFINITIONS AND CONCEPTS

Information Supports Decisionmaking

Information management characteristics are identified as follows:

- To be effective, decisionmakers must have the mental agility to render accurate decisions in recognition of existing social and political systems, customs, and norms.
- Information management is more than the sum of its three pillars and involves procedural improvements to incorporate technology and personnel requirements to support commanders and their organizational staffs.
- Effective information management must be a deliberate and proactive effort driven by commanders to align the actions of people enabled by technology to support the timely development of a common understanding of the environment.
- Information management is a C2 enabler and allows commanders to effectively convey guidance and direction to their staffs. Left unfocused, information management is just process refinement with no direction. Commander influence is essential.
- Information management contributes to better formulation and analysis of courses of action, providing both the right information for decisionmaking and execution as well as feedback/assessment on actions.
- Common understanding is the refinement of information using people, technology, and processes enabled by improved collaboration, concurrent planning, and focused execution.

By applying IM principles throughout the planning, decision, execution, and assessment cycle, commanders and staffs gain a more refined understanding of the elements of a dynamic battlespace faster. As stated in MCDP 6, "There are two basic uses for information. The first is to help create *situational awareness* as the basis for a decision. The second is to *direct and coordinate actions in the execution of a decision*." (emphasis added) Simply put, information is critical to the decisionmaking process and to the success of campaigns, operations, and tactical actions. Formally defining the concept of information management is necessary.

Information Management Defined

Joint Publication 3-0, *Joint Operations*, defines information management as "the function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals, and organizations in a way that optimizes access by all who have a share in that data or a right to that information."

Information management—

- Is the sum of the processes for the collaboration and sharing of information.
- Enables commanders to formulate and analyze courses of action, make decisions, execute those decisions, and adjust plans accordingly.
- Considers information a commodity.

Information management is more than control of data flowing across technical networks; it covers the entire lifespan of information and centers on commanders and their information requirements. Figure 2-1, on page 2-2, depicts the IM concept inside the well known OODA [observe, orient, decide, act] loop with C2 systems (technology) in the center, people on the outer ring, and IM processes as an enabler.

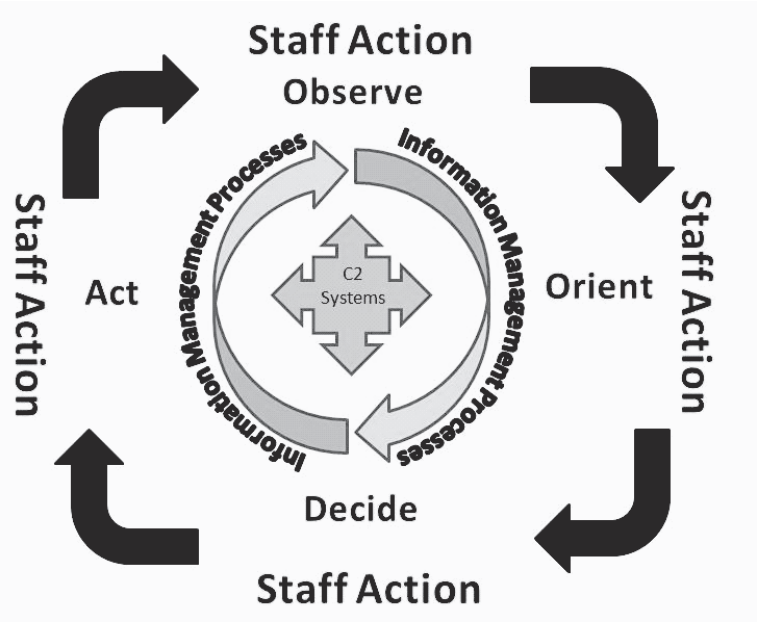


Figure 2-1. Information Management Concept.

Knowledge Sharing

As stated in Joint Publication 3-0, "Knowledge sharing complements the value of IM [information management] with processes to create an organizational culture that encourages and rewards knowledge and information sharing to achieve shared understanding. It supports team learning activities and a supporting environment. While information can be collected, processed, and stored as structured or unstructured content, such as in reports and databases, knowledge is acquired through a cognitive process and exists in the minds of individuals." Knowledge sharing, as it is referred to in this context, demonstrates an overlap of information management and the discipline of knowledge management.

Marine Corps Information Enterprise (MCIENT) Strategy calls attention for the need to institutionalize IM and knowledge management practices across the Marine Corps. Knowledge management is defined as the integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance. This definition is consistent with that presented in the *Department of the Navy Knowledge Management Strategy*. Beyond the scope of information management, knowledge management leverages the collective human, intellectual, social, and structural capitals to create knowledge-based organizations. Such organizations are aimed at accomplishing organizational goals and missions while sustaining a dynamic strategic advantage across the Marine Corps (see fig. 2-2).

The Relationship Between Information Management and Knowledge Sharing

Information management facilitates knowledge sharing as it relates to collecting, filtering, fusing, processing, focusing, disseminating, storing, and using information. Information is then internalized by the individual and fused with personal insights and experiences. As a result, tacit knowledge is brought to bear. Followed by episodes of socialization and collaboration, the free exchange of ideas forms the basis of shared understanding. The products of data, information, knowledge, and shared understanding are merged with the elements of situational awareness to render the wisdom needed to produce sound decisions. At the heart of this model is the integral merging of

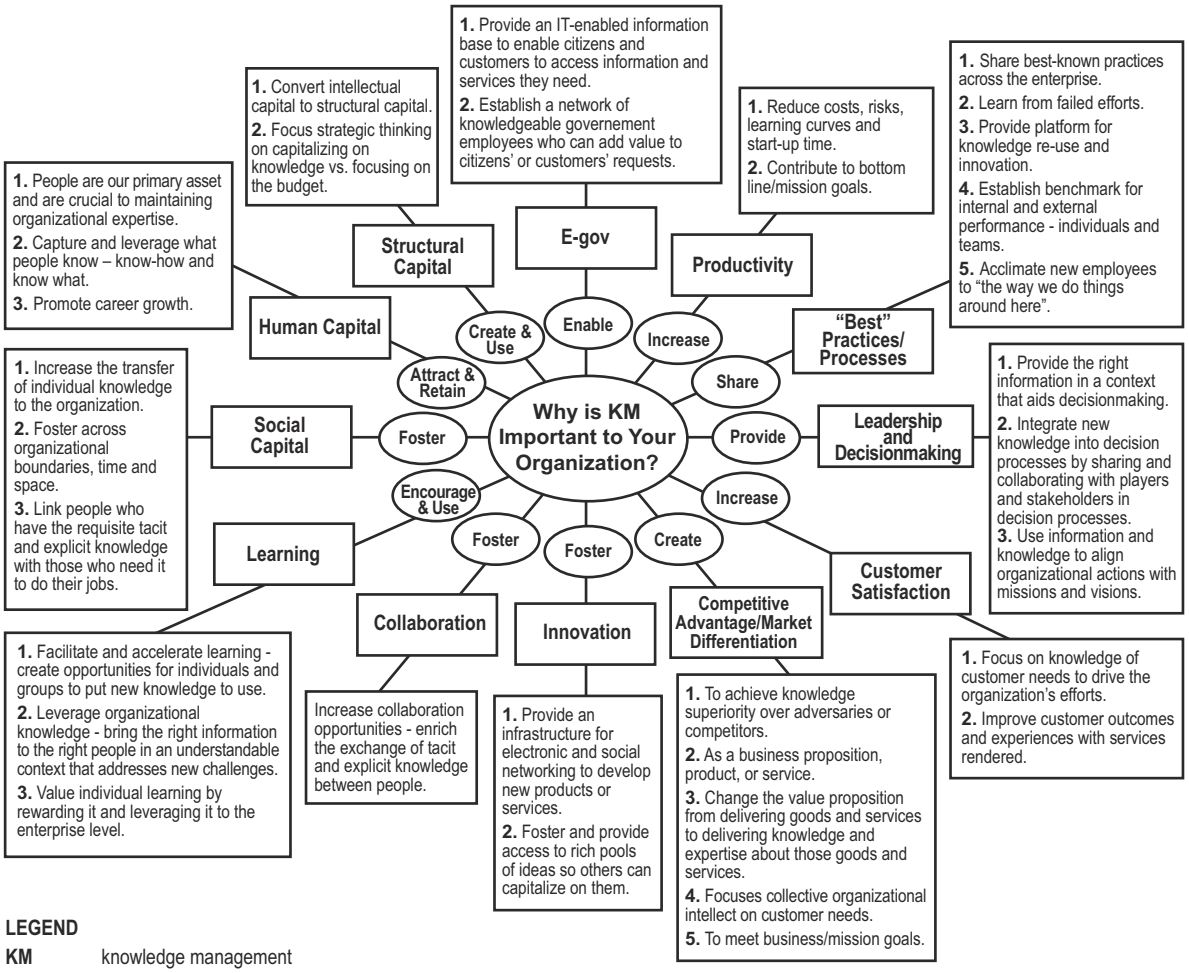


Figure 2-2. Importance of Knowledge Management to Your Organization.

information and knowledge. Without quality information management, the exchange of knowledge would be flawed and would degrade the decisionmaking outcome.

Creating Shared Understanding

Decisions are important products of the C2 function because they guide the force toward defined objectives and mission accomplishment. Commanders and staff use a balance of information and knowledge to develop the shared understanding that will provide the wisdom essential to sound decisionmaking. Shared understanding consists of five major categories: data, information, knowledge, understanding, and wisdom. Each category contributes to the decisionmaking process (see fig. 2-3 on page 2-4). The gradations between the different categories may not always be clear, but data becomes more valuable as it is refined and focused through the hierarchy.

Data

Raw data are the building blocks of processed information. Elements in this category are rarely meaningful until transformed and processed.

Information

Information is managed to frame its value and relevance throughout the hierarchy to eventually develop the commander's knowledge and understanding to improve his situational awareness.

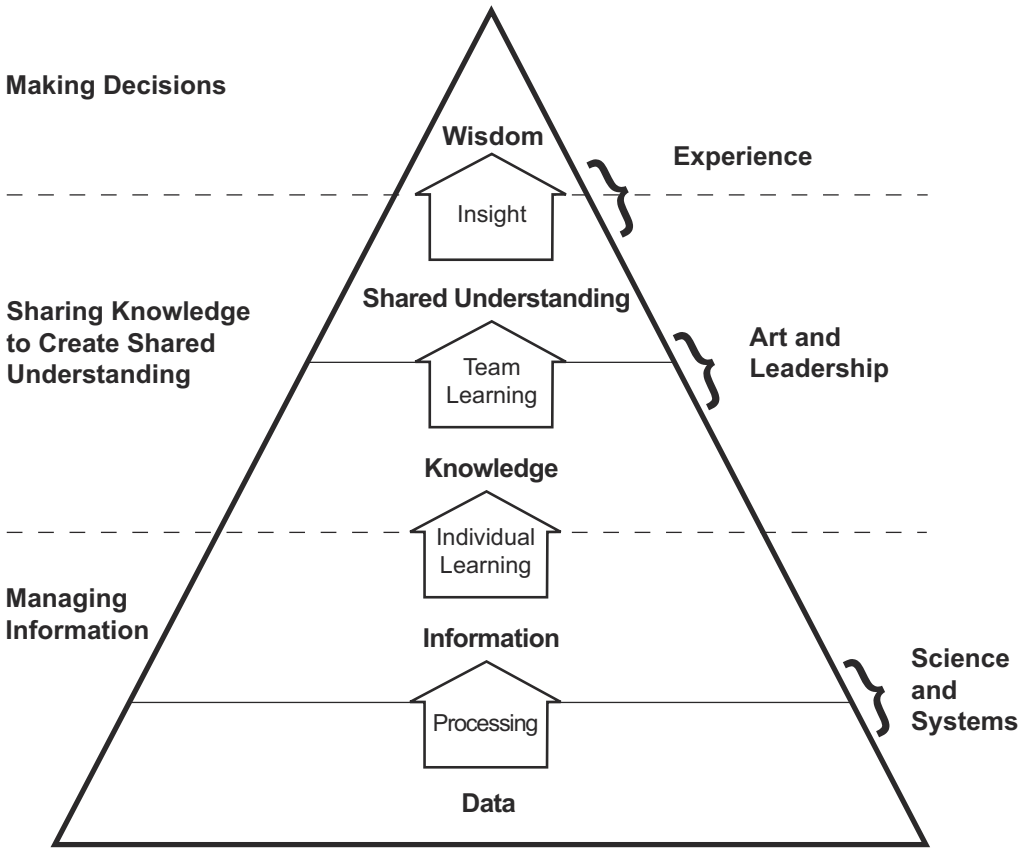


Figure 2-3. Creating Shared Understanding.

Information comes from organizing, correlating, comparing, processing, and filtering raw data, rendering the data understandable to the potential user.

Processing information can provide limited value. Processed data may have some immediate, tactical value, but it has generally not been evaluated or analyzed to determine its long term or operational significance.

Knowledge

Knowledge is required in order to—

- Exercise the human capacity (potential and actual ability) to take effective action in varied and uncertain situations.
- Understand a situation.
- Find meaning in a situation.
- Have insights into a situation.
- Create ideas related into a situation.
- Have intuition about a situation.
- Make effective judgments.
- Anticipate the consequences of some action.
- Recognize the who, when, where, why and how.

Knowledge includes facts, beliefs, truths and laws, concepts, methodologies, know-how, know-why, judgments and expectations, insights, relationships, leverage points, intuition and feelings, meaning, and sense making. Knowledge results from analyzing, integrating, and interpreting information; it provides value to an event or situation by linking and refining internalized information and data. Types of knowledge can be further defined as explicit or tacit.

Explicit Knowledge

Explicit knowledge can be called up from memory and put into words and shared (also called declarative knowledge). Often, it is placed into standing operating procedures, lessons learned, intelligence reports, standing orders, and

contingency plans. This knowledge can be organized, applied, and transferred in digital or nondigital form. It lends itself to understanding rules, limits, and other precise meanings, and allows an individual to develop and understand his personal world views or mental models.

Tacit Knowledge

Tacit knowledge only resides in an individual's mind. It is knowledge formed by those connections that cannot be pulled up from memory and put into words. The implicit form of this knowledge is often pulled or triggered by memories and portrayed as our visceral reactions to certain stimuli. In the metaphysical sense, it is a person's ability to perform fine motor functions or even walk. All individuals have a unique store of experience gained through life, training, and education and can be impacted by formal and informal social networks. Even though tacit knowledge cannot be readily described by the individual it can be observed through role-playing, mentorship, and analyzing situational outcomes. If it is documented or verbalized, this tacit knowledge can be used as a form of explicit knowledge creation to be shared and promoted to enhance education and training.

We develop tacit knowledge by internalizing explicit knowledge through practical application, feedback from experienced practitioners, and through personal reflection. One notable example of this technique is the observe, orient, decide, act loop. Once observed and identified it can be trained and practiced to develop one's immediate responses in given situations.

Understanding

Understanding provides context or framing of knowledge. Understanding is an appreciation for not just what is happening, but, more importantly, why it is happening. Understanding results when knowledge is combined with experience, judgment, and intuition in a collaborative environment. Collaboration and debate allow decisionmakers the opportunity to reduce gaps generated by uncertainty and to apply insights and situational awareness fully in order to arrive at a complete mental image of the situation.

Wisdom

Once understanding and clarity of the mental image is achieved, the commander is able to better anticipate future events and make sound decisions, even in the face of uncertainty. These distinctions are critical to refining an understanding and value of information management. While data and information can be created and handled without human intervention, knowledge and understanding explicitly require human involvement. To create knowledge, an individual must participate in the process and move processed data from the physical to the cognitive realm. To create understanding, he must integrate knowledge with judgment and experience. While knowledge exists at the boundary between the physical and cognitive realms, understanding exists only in the cognitive realm.

Information Quality Characteristics

Quality information adds value to the decision-making process. In the face of uncertainty, information managers must consider the information quality characteristics outlined in table 2-1.

Table 2-1. Information Quality Characteristics.

Accuracy	Information conveys the true situation
Relevance	Information applies to the mission, task, or situation at hand
Timeliness	Information is available in time to make decisions
Usability	Information is in common, easily understood formats and displays
Completeness	All necessary information required by the decisionmaker is available
Brevity	Information is succinct, but at the level of detail required
Security	Information is afforded sufficient protection where required

Situational Awareness

Situational awareness is the knowledge and understanding of the current situation that promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. (Marine Corps Reference Publication 5-12C, *Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms*) Situational awareness includes:

- Understanding of the physical environment.
- Comprehension of people's purposes and movements relative to their physical environment.
- Ability to anticipate the impact of future actions within the environment.

Some level of situational awareness can be achieved with information, but it tends to improve as information is refined and processed into knowledge and understanding through the cognitive hierarchy. As available information is refined, situational awareness is improved, which enables commanders to better anticipate future conditions, visualize courses of action, provide guidance, and accurately assess outcomes. Developing situational awareness with limited and uncertain information under pressing time constraints is one of the fundamental C2 challenges.

There are two fundamental aspects of situational awareness: information and skill. The staff and subordinate unit commanders provide the information component and feedback to build situational awareness. The skill component is based on the commander's personal experience, judgment, and intuition combined with his ability to assimilate and understand the surrounding environment. The combination of information and skill provides the commander with an image of the situation from which he can base decisions.

Shared Situational Awareness

Shared situational awareness is the commander's conveyance of operational intent and assessment of a situation to distributed organizations in order to influence efforts of the organization and to guide the outcome of operations. Shared situational awareness requires the alignment of command and control so information is readily shared, providing commanders with common near-real-time information on which to base decisions. The concept impacts the development of C2 systems and processes in order to provide commanders with the agility required to quickly respond to situations. The concept of shared situational awareness impacts IM best practices and, thereby, technology.

Neither knowledge nor understanding can exist without an individual assimilating and processing information. Knowledge clearly requires that an individual process and analyze information. Understanding requires an individual to assimilate information, elevate it to knowledge, then apply judgment and experience to fill gaps and form a mental image. Information managers must seek to deliver information in forms that facilitate and accelerate sharing, knowledge, and understanding.

CHAPTER 3
INFORMATION MANAGEMENT PERSONNEL AND DUTIES

Duties and Responsibilities

People comprise the second element of command and control and the most crucial pillar of information management. It is the people who push and pull information and leverage collaboration tools that ultimately allow commanders access to quality information for timely decisions.

This chapter identifies the principal information managers and outlines their responsibilities. Information management exists to improve information flow by using technology to better integrate people and processes. Consequently, if commanders are responsible for their C2 systems and IM processes, then they must understand C2 and collaborative systems, the impact C2 systems have on information flow, and the responsibilities people have for producing essential information products. Commanders must further understand that there are many contributors to the development of products, which can contribute to the complexity of the C2 solution. Technical and operational relationships and responsibilities must be properly aligned and coordinated for timely information refinement, production, delivery, and consumption. Defining the duties of key personnel establishes their relationship to IM functions and highlights their contribution to effective information flow.

Although certain individuals are labeled as key personnel with specific IM-related duties, every member of a command has an inherent responsibility to assist with the functions of collecting, managing, filtering, fusing, disseminating, protecting, and storing information. In a personnel-constrained environment, IM personnel may serve multiple roles and provide expertise to numerous functional areas, such as boards, bureaus, centers, cells, and working groups (B2C2WGs) and staffs. In every command, information users must support IM procedures to enhance the flow of information and the generation of knowledge and understanding.

An organizational chart, battle roster, operational battle rhythm, C2 system diagram, and list of information exchange requirements (IERs) are products normally developed to align a military organization and its C2 for operational effectiveness. A clear benefit to a detailed C2 planning process is the highlighting of individual responsibilities.

Figure 3-1, on page 3-2, depicts the relationships between information managers and key command/battlestaff personnel. It highlights the critical need to coordinate people, processes, and technology to support and integrate battlespace awareness, mission readiness, and command decisionmaking.

The information management officer (IMO), working for the chief of staff (C/S) or executive officer (XO) at lower echelons, develops and refines the processes and procedures necessary to harness information for the command and guide daily staff actions (see fig. 3-2 on page 3-2). The IMO works with staff section information managers to understand, facilitate, and improve information flow. Critical to the IM processes and procedures is the underlying network-centric communication architecture and hardware, provided by the G-6 or S-6, and the staff section/subordinate unit information manager's understanding of his particular C2 system or application.

Relative levels of effort are reflected in figure 3-3 on page 3-3. Although key personnel with specific IM duties are important, all information users have a duty to facilitate information management and support knowledge-based decisionmaking. Every

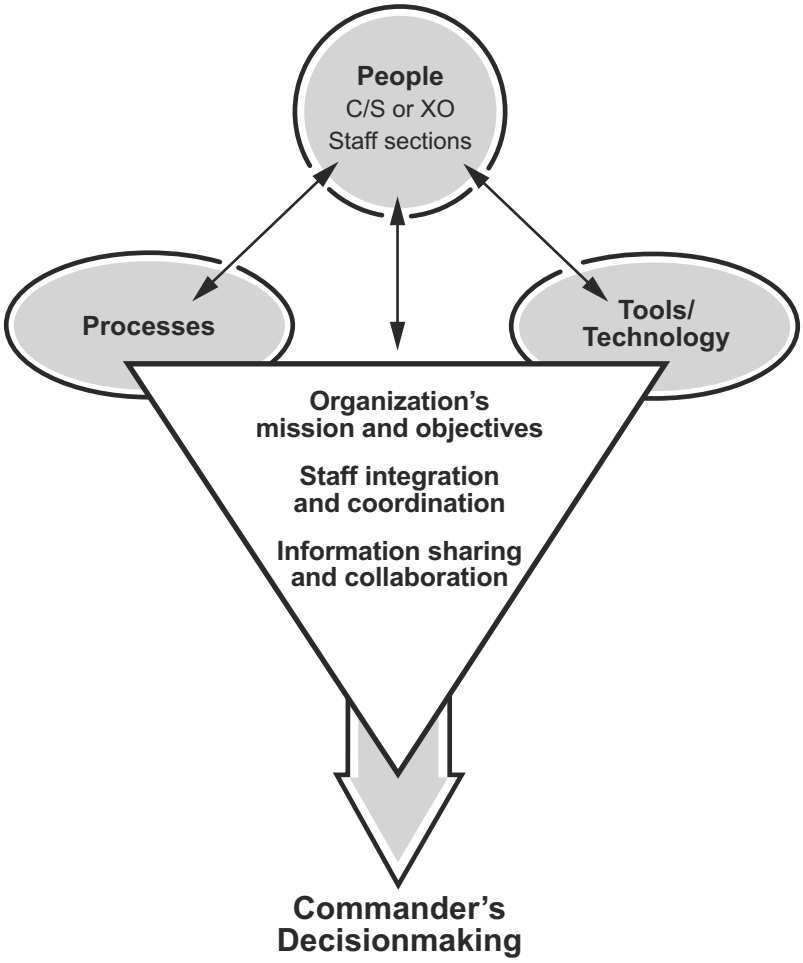


Figure 3-1. People, Processes, and Technology in Support of Commander's Decisionmaking.

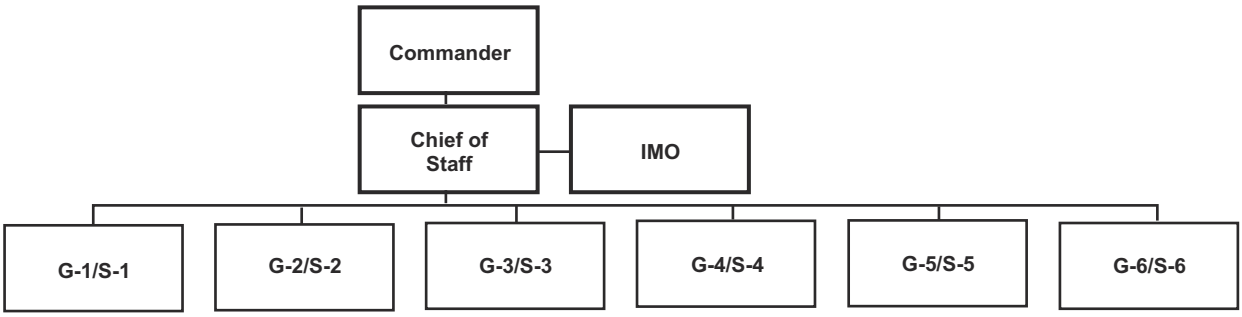


Figure 3-2. Staff Organizational Chart.

user has an inherent responsibility to filter and fuse information for personal use and for use by others. Every user also has a duty to protect sensitive information. All personnel, as information users, support IM procedures that enhance decisions made throughout the decision cycle.

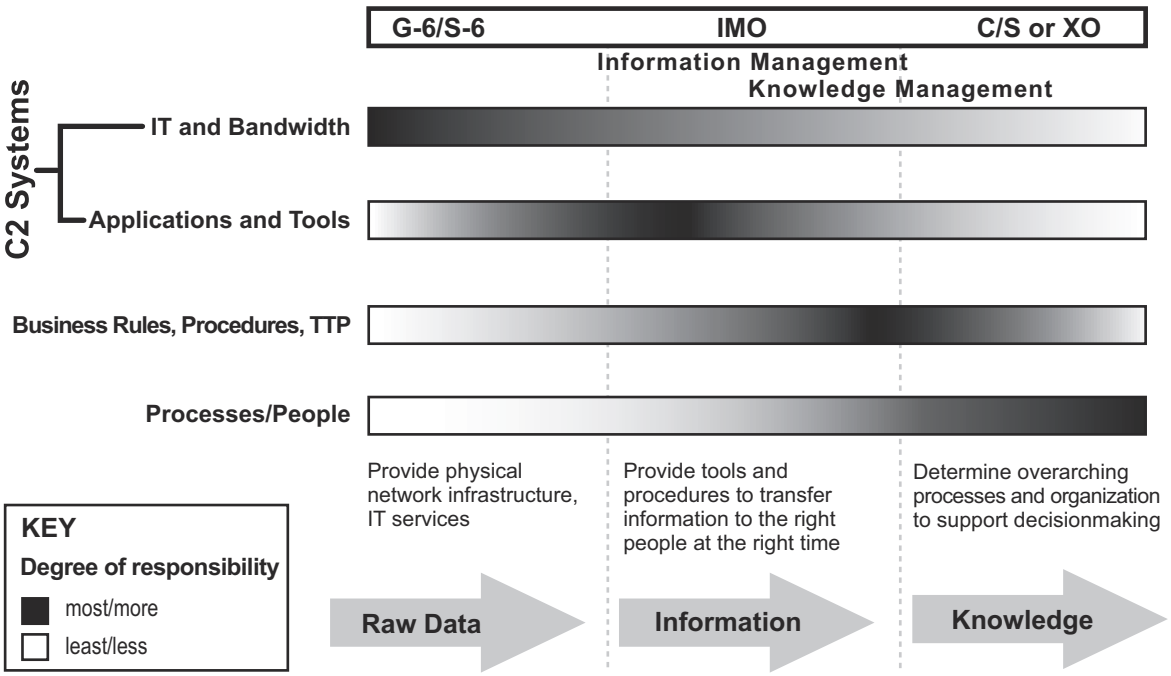


Figure 3-3. Levels of Responsibility.

Key Information Management Personnel

Commander

The commander aligns command priorities and drives the planning process. Commander's intent and guidance are foundational elements to planning and execution. The commander uses the Marine Corps Planning Process to gain understanding and situational awareness to support decisionmaking, establishing priorities for gathering and reporting information. Clear guidance, commander's intent, and commander's critical information requirements (CCIRs) enable the staff to focus on identifying information used to support and make key decisions. The commander performs the following IM functions:

- Sets expectations for staff and subordinate command knowledge and information needs, including defining acceptable shared situational awareness.
- Provides commander's guidance for information management.
- Approves command information management plan (IMP).
- Approves command communications plan that complements and supports the IMP.
- Develops and approves CCIRs.

Chief of Staff or Executive Officer

The C/S or XO is responsible for coordinating staff actions and ensuring the commander is provided necessary information to make informed decisions. As the principal supervisor of staff processes, the C/S or XO is uniquely positioned to view and influence the process that binds the staff into a cohesive and productive organization. The C/S or XO performs the following IM functions:

- Appoints and supervises the IMO.
- Implements the IMP by providing the mechanisms to coordinate the staff.
- Directs development of and approves the battle rhythm.
- Appoints and assigns leadership and responsibilities to B2C2WGs.

- Ensures IM procedures yield the quality and actionable information needed to support the commander's decisionmaking process.
- Ensures information is properly classified and that steps are in place to protect sensitive information.

Principal Staff

Principal staff members are the eyes and ears of the commander. The staff receives the commander's guidance, intent, priorities, and CCIRs. The staff uses such direction to collect, filter, and analyze data into focused and processed information, knowledge, and understanding for the commander. Principal staff members perform the following IM functions:

- Appoint a staff section information manager as a point of contact for IM matters.
- Appoint personnel responsible for maintaining section-specific information technology (IT) and network infrastructure used to share quality information.
- Identify pertinent information and activities used to support the organization battle rhythm.
- Establish internal staff section procedures with concurrence from the IMO to share quality information through the use of appropriate technologies, requests for information, and suspense control measures.
- Ensure basic IM training is completed for appropriate personnel in each staff section.
- Evaluate IM procedures to assure efficient flow of quality information.
- Establish benchmarks and subjective analysis to evaluate efficiency and effectiveness of IM procedures in support of knowledge-based decisionmaking.
- Work closely with the IMO to develop architectures that identify functional tools, applications, procedures, and processes required to share quality information with those who need it in a format that is clearly understood.

At times, the staff may be called to work in a coalition/joint environment wherein the flow of information will be from different sources.

Information Management Officer

The IMO works closely with all personnel within the command and in joint, coalition, or multinational environments to develop and coordinate procedures necessary to share information. The IMO facilitates the flow of information, synchronizing C2 technologies and battlespace-function-specific technologies through the IMP. Information management processes and procedures must promote development and exchange of information required by the commander, staff, and unit personnel in order to make informed decisions consistent with the commander's intent. The IMO must be aware of the following:

- Key decisions the commander is expected to make to successfully achieve desired results. Such decisions are normally reflected in CCIRs and decision support matrix (DSM).
- Information that is required to set conditions for tactical operations, is needed daily to maintain commander situational awareness, and is provided in daily reporting.
- Information required by the commander to reduce uncertainty about his force, the enemy, and the environment. Such information must be provided to the commander in a format that promotes understanding to make sound, timely decisions to satisfy CCIRs.

To perform the functions listed above, the IMO—using the IM staff—must accomplish the following tasks:

- Develop and publish the command IMP and/or corresponding IM annex or appendix to operation orders (OPORDs) or plans.
- Determine IERs that impact networks, systems, and applications required to plan for and integrate collaborative and C2 systems.

- Publish and update the reports matrix.
- Develop the daily battle rhythm and support/facilitate B2C2WG collaboration.
- Coordinate additional training required by staff and component elements to support production of quality information through effective IM procedures.
- Ensure effective information exchange throughout the Marine air-ground task force (MAGTF). Work closely with staff principles, staff section IM representatives, and subordinate and higher headquarters' IMOs to ensure IM procedures and processes are published and understood.
- Ensure that recommended information flow improvements/enhancements are brought to the C/S or XO for evaluation and possible implementation; prepare/coordinate plans for any changes to established IM processes and procedures.
- Determine metadata requirements for information to allow for quality "enterprise" search for information.
- Support continuous process improvement within the command.

Staff Section Information Managers

Staff section information managers facilitate IM procedures and must be aware of what information is required by the commander, when it is required, and how it should be formatted. Section information managers are expected to perform the following tasks:

- Monitor the information flows and processes to, from, and within their respective staff sections.
- Ensure the command IMO is aware of information produced by each staff section to satisfy CCIRs. Provide routine daily updates that the commander requires to make informed, timely decisions.
- Provide G-6 or S-6 daily updates of command level information development and sharing requirements that may need network infrastructure and equipment to support functional needs.
- Ensure compliance with IM procedures used to share information on e-mail, chat, data storage/access, and other network capabilities.
- Coordinate and conduct IM training for internal staff section members.

Request for Information Manager

Requests for information (RFIs) are questions that cannot be satisfied by organic staff personnel. Requests for information are consolidated among the staff and forwarded to higher headquarters (HHQ). The RFIs are staff-to-staff interactions designed to facilitate an explicit response, usually within an agreed upon time frame. Responses to RFIs are shared with the requestor and staff to promote the understanding required to support the commander and to reduce uncertainty within the command. The following tasks are performed by RFI managers:

- Receive, validate, prioritize, and submit RFIs to the appropriate authority for resolution.
- Develop and manage RFI tracking systems to ensure RFIs are processed and responses are expeditiously disseminated to the requester and made accessible to all personnel.

Common Tactical Picture Manager

The common tactical picture (CTP) manager is responsible for reporting and displaying situational awareness information including friendly and enemy unit tracks. An accurate, integrated tactical or operational picture is valuable in that it displays near real time unit location, intelligence, and operational information using a standard symbol set. A properly managed CTP provides a visual depiction or model of the operational environment, allowing commanders to proactively assess and control the subordinate actions for a predictable outcome. The CTP is crucial to the

concept of shared situational awareness. The CTP manager is responsible to:

- Understand and follow combatant commander common operational picture (COP) reporting and management guidance and policy.
- Coordinate/deconflict all tracks from all sources with all major subordinate commands (MSCs) and HHQ using joint standard automated data formats.
- Work closely with senior watch officer (SWO) and relevant picture providers to ensure the location and disposition of friendly and enemy ground units is visually updated as required. Emphasize the proper use and deconfliction of automated position location information data.

Portal Master

Internet/intranets are valuable resources used to share quality information within and external to the staff. Creating and maintaining a unit Web site or portal is the responsibility of the portal master. Specifically, the portal master is responsible to:

- Create command portals to support information sharing. The portal should support internal and external reporting requirements, CCIRs, RFIs, and the commander's daily brief and daily battle rhythm.
- Maintain portals to ensure changes to information requirements are posted in a timely manner and ensure information contained therein is available to appropriate personnel.
- Maintain access to portals and information in deployed environments.
- Ensure procedures are developed, disseminated, and understood for access, information upload, and updates/changes.
- Advise and assist staff section portal representatives, develop formatting standards, create initial pages for each staff section, and provide training to help maintain uniformity of design between sections.
- Maintain links to external portals or sites of interest to the staff, developing custom applications as required.

Subordinate Unit and Higher Headquarters Information Management Officers

Each MSC and HHQ appoints an IMO as a primary point of contact for IM matters. Subordinate and HHQ IMOs can be expected to perform the following tasks:

- Review/update information reflected by the reports matrix and daily battle rhythm to subjectively assess the procedures and processes that are used to share information for decision-making. Conduct liaison with the HHQ and adjacent IMOs.
- Coordinate and assist personnel training required to produce quality information throughout the MAGTF.
- Ensure appropriate IM personnel are designated within the command to address technical support for MAGTF wide automated and electronic command information sharing means, such as CTPs, Web sites, wikis, blogs, public folders, and shared directories.

Information Management Coordination Boards, Bureaus, Centers, Cells, and Working Groups

To ensure IM procedures are in compliance with those established by a joint task force (JTF), IM B2C2WGs in appropriate organizational configuration are recommended at the MAGTF and component levels. Such B2C2WGs may also be established at lower levels of command and are convened to facilitate coordination among users, service providers, and technology maintainers as required. A board, bureau, center, cell, or working group may also be activated at the JTF to enable IM procedures at the component level.

Information Management Board

The IM board is the focal point for coordinating IM issues within the command. It convenes during

the development of the IMP and as required thereafter. The IM board operates under the supervision of the C/S or XO or the appropriate staff directorate to meet the commander's mission needs. Facilitated by the command IMOs, it is composed of the senior IMO from each MSC and IMO representative from appropriate staff sections. The IM board is actively involved in resolving cross-functional and contentious IM issues. Personnel who administer information exchange technologies (i.e., G-6 or S-6 personnel) also attend.

Common Tactical Picture Board

The CTP board acts as the focal point for coordinating the CTP within the command. It is convened by the CTP manager who is responsible for working closely with the IMO, the primary battlestaff, and subordinate and HHQ IMOs to develop CTP procedures to maintain a near real time picture of friendly and enemy forces. The CTP board operates closely with appropriate staff sections, IMO, combat operations center (COC), and combat intelligence center watch officers. It is composed of the friendly air, land, maritime, and enemy force track managers and is actively involved in resolving all cross-functional CTP issues. All personnel must take appropriate actions to safeguard information.

Information Security Personnel

While the personnel filling the billets of foreign disclosure officer, information security manager, special security officer, information assurance manager, information assurance officer, and operations security officer do not work for the IMO, they are integral to the command's management and security of its information and information systems. In some cases, the IMO may appoint or be assigned personnel to coordinate with the G-6 or S-6 on information security issues.

Foreign Disclosure Officer

Military information is a national security asset that must be protected. Sharing information with foreign representatives within a coalition environment is complex and it is further complicated by national and international law, treaties, and alliances. Only designated foreign disclosure officers may approve the disclosure of classified military information and controlled unclassified information to foreign representatives.

Information Security Manager

The information security manager is responsible for the proper accountability, control, personnel access, and physical security/storage of noncompartmented classified data that is in both hard and soft copy forms. This includes the top secret control officer's responsibility for the JTF top secret registry's accountability, control, and access.

Special Security Officer

The special security officer is responsible for sensitive compartmented information management, control, and access. This function is typically executed by the G-2 or S-2.

Information Assurance Manager

The information assurance manager (IAM) is the primary staff officer charged with computer network defense. The IAM develops plans, policies, and procedures to ensure the reliability, availability, integrity, confidentiality, and protection of data and information as well as to verify the authenticity and nonrepudiation of personnel accessing such data and information. As a member of the G-6 staff, the IAM's primary responsibilities include information assurance as well as the following:

- Managing network security.
- Detecting intrusion.
- Assessing vulnerability.
- Assisting in the network accreditation process.

Information Assurance Officer

The information assurance officer is responsible for safeguarding the information systems of the command. This is done by conducting site surveys and accrediting systems to process classified and sensitive information. The information assurance officer also enhances the information security knowledge, skills, and abilities of the command through education and training programs. The information assurance officer performs the following IM functions:

- Develop/maintain a plan for site security.
- Ensure the information system is operated, used, maintained, and disposed of in accordance with security policies and practices.
- Ensure the information system is accredited and certified if it processes sensitive information.
- Ensure users and system support personnel have the required security clearances, authorization, and need to know; are indoctrinated; and are familiar with internal security practices before access to the information system is granted.
- Enforce security policies and safeguards on all personnel having access to the information system for which the information systems security officer is responsible.

Operations Security Officer

The operations security officer is responsible for oversight and implementation of the command operations security program, ensuring the protection against compromise of friendly force information. This position is normally a G-3 or S-3 function and will receive support from the G-2 or S-2 (counterintelligence officer).

Information and Information System User Responsibilities

It is incumbent upon all users of information to ensure the proper flow of information. The duties and responsibilities of users of information and information systems are identified in the following list:

- Report information as required by the command CCIR.
- Ensure accuracy and relevance of information before further dissemination. Clearly differentiate between original information and previously reported information to avoid duplicative reporting.
- Ensure all individual information assurance training and required security clearances are current. Coordinate required authorizations and need to know, system indoctrination, and internal security practices with the information assurance officer before access to the information system is granted.
- Properly control, classify, protect, and archive all information and information systems for which they are responsible. This requires a clear understanding of approved control measures for various classifications of information.
- Read and comply with the information requirements published by the IMP.
- Properly control information throughout the entire information lifecycle, including proper disposal. When conducting an initial analysis and correlation of data, set aside but do not destroy irrelevant or conflicting data. This information may become useful when combined with additional facts.
- Continuously pull and push information (see fig. 3-4); provide information to those that need it, when they need it.

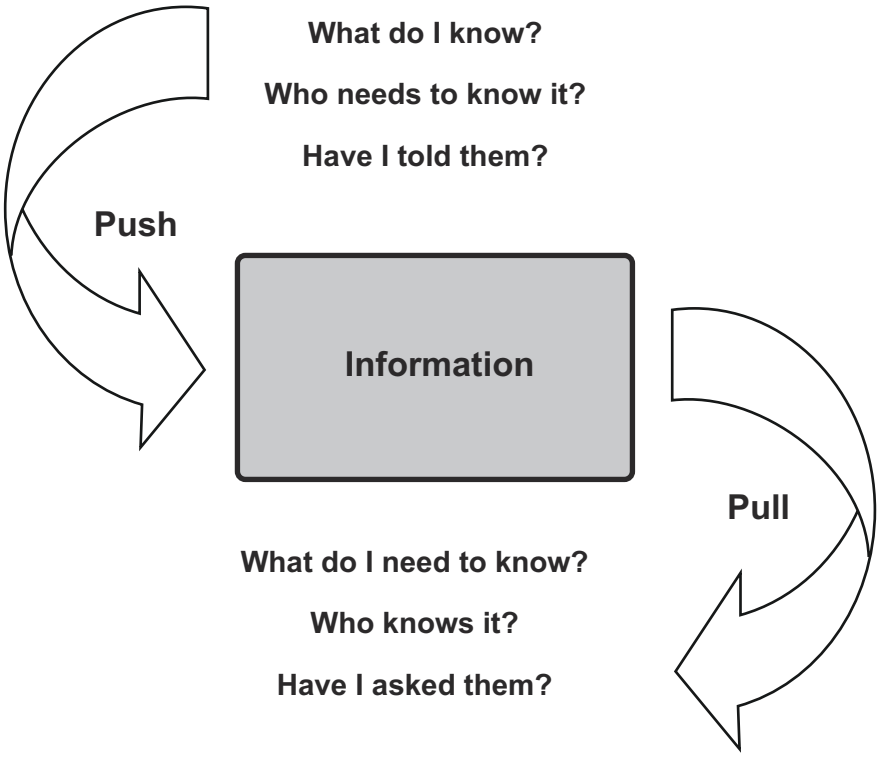


Figure 3-4. Information Push Pull Concept.

This Page Intentionally Left Blank

CHAPTER 4
INFORMATION MANAGEMENT PROCESSES AND PROCEDURES

Information management processes and procedures are not solely defined by advanced technology and equipment—they are the integrated use of organizations, people, capabilities, training, doctrine, and network infrastructure to support command and control and decisionmaking. This chapter discusses principles, processes, and procedures that improve command and control.

Information management processes combine the commander's information needs, the associated products, and C2 systems. These processes contribute to the purposeful, continuous, uninterrupted flow of information throughout the organization. Because of the proliferation of complex C2 systems and resulting increased volume of data and information, commanders and staffs must process and manage information very deliberately. Today's operational processes require staffs to consider the rhythm of the operational action, impact of technology, flow of information, and schedule of personnel involved to facilitate and coordinate command and control. The alignment of technology, people, and focused processes is a visible C2 enabler. The information management process considerations include the following:

- What information is critical to the commander and when is it needed?
- What format and style is required by the commanders?
- Who is responsible for obtaining, processing, analyzing, correlating, and disseminating the information?
- How should this information be protected and from whom?
- Does the required information already exist?
- Who else might need the information?
- Who has the need to know?
- Who has authority to release information?
- What is the best way to effectively get the information to other users?

Information Management Principles

Information management principles frame C2 solutions. The principles discussed in the following subparagraphs provide a foundation for shaping and prioritizing IM activities. They are relevant regardless of the situation or mission.

Define the Information Flow with Prioritized Requirements

Command relationships, force organization, mission, and information requirements influence the flow of information. The following are crucial to proper information flow:

- Identify and prioritize information requirements.
- Ensure resources are available and tasked to collect and provide the prioritized information to the intended audience.
- Coordinate personnel, equipment, training, procedures, IT, and communications to ensure information is available to the decisionmaker when needed.

Seek and Deliver Quality Information

Information must be accurate, complete, and relevant in order to obtain knowledge and understanding. To accomplish this, information requirements should be determined as early as possible in the process.

Sufficient resources should be employed to obtain the data and to process, collate, and synthesize the information. As information becomes knowledge and understanding through processing, it can be framed within context and for the commander's use in decisionmaking. As situational awareness is gained and maintained, less repetitive information is required in briefings, freeing time for discussion and collaboration.

Based on the commander's information requirements, repetitious information should be set aside but not discarded. Further, care should be taken to retain data that may be relevant to future decisionmaking or analysis.

Use Multiple Sources of Information

Using multiple redundant sources to gather and process data helps validate findings on the battlefield by allowing a venue to compare collected information and identify discrepancies. Ideally, three or more sources might highlight a single, inaccurate data source for rapid exclusion. Too few sources can make it difficult to disregard inaccuracy, potentially allowing good data to be questioned. Too few sources can also cripple decisionmaking: because one source may discredit another and, without enough corroborating information, the commander may be forced to make a subjective call or delay decision. If only two sources are available and they conflict, the best choice may be to avoid using the information until its accuracy is further verified. Best practices include establishing metrics for credibility and noting noncredible information sources.

Deliver Timely and Usable Formats

Information delivered late is of no value to the decisionmaker; the time for decision having passed. The goal is to deliver the information that is available when it is needed and in a form that is readily understandable to the commander for decision. Known gaps in the information should be properly characterized and a forecast for when more relevant data will become available should be provided. There is a dilemma in decisionmaking when clarity or availability of information is not adequate and the commander must assume a risk. Making no decision or delaying a decision also increases risk.

Identify and Trap Errors

Procedures must be in place to identify sources of errors and to trap those errors through procedures that compare, validate, or verify data accuracy throughout its lifecycle, particularly when used in mission-critical or safety-of-life processes or applications. This is especially important when unstructured and nonsecure information exchange mediums are employed. A common example is sending coordinates using e-mail or text collaboration—for example, characters are easily transposed while entering or recording the information (both of which represent error entry points). In such a case, a process to plot and validate these coordinates before their use is essential.

Protect Information Throughout its Lifecycle

Information is at risk from the moment it is collected until it is no longer of any value; moreover, the nature of the threat to that information varies throughout the information lifecycle. Potential threats include not only overt actions on the part of external actors, but also failures on the part of data owners to properly implement and manage the information through its lifecycle.

Build Understanding from the Bottom Up

The nature of recent conflicts has forced a refocus and reconsideration about the value of, priority of, and effort invested in information. Warfighters must now attempt to make sense of the actions of many actors, whether they are the enemy or those operating according to other interests. Their actions and intentions may be those of external elements, political leaders, tribal or local elders, insurgents, and noncombatants.

Often, the best information will come from the many "strategic corporals" who have boots on the ground. Information management processes must support these contributors and capture their situational awareness to provide understanding at the operational and strategic levels.

Decentralize Information Management Execution

In order to maximize the ability to reliably and rapidly process and disseminate information to the intended audience, IM activities should be decentralized to the greatest degree possible while maintaining effective control. Though technology by its nature is centralized, centralization of IM activities creates bottlenecks that restrict information flow. These bottlenecks occur when too much information is delivered solely to a key node (whether people or technology) and result in backlogs for information processing and dissemination.

Reduce Complexity

While complexity cannot be avoided completely, it must be minimized so that people can *focus on the information* rather than on the tool or devices being used to *present the information*. Complexity has the following results:

- Higher expenditures for initial and sustainment training.
- Lower proficiency if the training effort is inadequate.
- Higher probability that the data will initially be misinterpreted or unusable by decisionmakers.

Aligning commander expectations with investment in process development, user training, and system integration will focus technology capabilities for the intended outcome.

Tailor Information for Intended Audience

Information increases in value when formatted or tailored for the audience. Tailoring presentations and visualizations accelerates the process of moving from raw data to decisionmaker understanding. On the other hand, general or unformatted information frustrates and delays decisionmaking, requiring leaders to translate data into a consumable format to achieve understanding before critical decisions can be made.

Set Conditions for Information Development and Sharing

The ultimate goal of information management is to provide a process to enable the user to leverage C2 systems that empower personnel with relevant skills to understand and shape battlespace (see the battlespace clearly) and recognize, collect, and share critical information with decisionmakers in order to defeat opponents. Creating conditions for rapid information sharing and its resulting assimilation of knowledge for decisionmaker understanding requires more than production, transportation, and presentation of volumes of data. It requires the establishment of a culture within the force to receive and rapidly process relevant data. Such a force must have a keen understanding of the collaborative and C2 systems that model the battlespace; share, store, and visualize information; and provide context for decisionmaking. Information management must enable users to accomplish the following:

- Be aware of available resources (C2 systems) that find and retrieve relevant information—the higher the quality and timeliness of delivery, the greater the value.
- Institute a culture of information and knowledge sharing with a sense of urgency and a keen sense of understanding.
- Ensure every leader from fire team leader up is assigned commensurate responsibility for preparing, presenting, and ensuring delivery of high-quality training and information sharing to subordinate Marines.
- Ensure personnel are provided C2 system learning opportunities through high-quality training

events. Proactively plan appropriate technical and process resources as required for effect.
- Ensure new information relevant to the unit's mission and training objectives is rapidly incorporated into existing training throughout the training cycle. Information sharing is a continuing action.

Enabling Command and Control System Structure

Information management is a C2 enabler and must work inside C2 infrastructure. Technology capability is balanced by information sharing policy and technical limitations. The following concepts define C2 architectures and nuances in a hierarchical form to allow users to leverage technology capabilities in a military context.

Effective Command and Control Structure

An effective C2 structure provides the benefits of labor and time savings and ease of dissemination and information flow.

Capabilities and commonly understood procedures enable the performance of intensive calculations very quickly that otherwise might take several people much longer to complete. Networked C2 structure capabilities allow users to transfer information and knowledge simultaneously to many users even if they are not in the same geographic location. Further, when enabling a C2 structure to enhance the flow of information across warfighting functions (maneuver, fires, logistics, force protection, intelligence, and command and control) and across traditional staff section boundaries, the factors discussed in the following subparagraphs should be considered.

Location of Information

The location for specific types of information is often predictable, especially if the process to support the information requirement is understood. Prepositioning required information at anticipated point(s) of need speeds up the flow of information, reduces demands on communication networks, and provides required information to those who need it in a timely manner. This consideration is especially important when units are highly dispersed.

Mobility

Reliable and secure flow of information must be commensurate with the commander's mobility and tempo of operations requirements. Capabilities and procedures necessary to support effective information flow must be flexible enough to adjust immediately in order to support bandwidth challenged and highly mobile command posts, as well as the mobility requirements of the subordinate units.

Accessibility

All levels of command must have access to the information they require to support concurrent/parallel planning, mission execution, and assessment. The IM structure provides access to information to required user(s) via automated means to reduce time and confusion while increasing efficiency and dissemination of quality information (e.g., automated, dynamic visual displays of force).

Push Versus Pull

Information management uses two basic approaches to share information—supply push and demand pull. The IM structure must incorporate the most appropriate approach based on the commander's information requirements.

A supply push methodology relies heavily on information being pushed from the source to the user, either as the information becomes available or according to a schedule. The advantage of supply push is that the commander does not need to request quality information. Quality information is delivered to the user in a timely manner, but there is always the danger of information overload because producers of information may not completely understand user information requirements (e.g., daily intelligence summary).

In contrast to supply push, a pure demand pull system requires the user to initiate the flow of information, seeking out information required. If the information is readily available (already resident in some database), the requirement can be quickly satisfied. If not, the requirement must move through the chain of command until it reaches the appropriate level. Information can be tailored specifically to support the identified requirement, avoiding overload. The disadvantage to demand pull is the potential increase in time, since the search for information may not begin until the commander or user has identified the need (e.g., RFI systems).

Networks

Numerous systems or applications are used to support operational requirements. The information generated and personnel using these tools may, however, require different communications networks for information sharing and dissemination. A brief explanation on several of the most common networks is provided in the following subparagraphs.

Sensitive Compartmented Information Networks

Specific classified networks are used to process and disseminate information classified as sensitive compartmented information. These networks include the Joint Worldwide Intelligence Communications System and the National Security Agency Network.

SECRET Internet Protocol Router Network

The SECRET Internet Protocol Router Network (SIPRNET) is a classified network that is authorized to process and disseminate information classified as SECRET or below.

Nonsecure Internet Protocol Router Network

The Nonsecure Internet Protocol Router Network (NIPRNET) is a sensitive but unclassified network that is able to process and disseminate sensitive but unclassified information and below.

Coalition Wide Area Network

There are three aspects of the coalition wide area network: the Releasable Internet Protocol Router Network, the Combined Enterprise Regional Information Exchange System (CENTRIXS), and the All Partners Access Network.

The Releasable Internet Protocol Router Network is a secure coalition network used for joint, Republic of Korea, and United States usage.

The CENTRIXS is a combination of global, multilateral, and bilateral, virtually separate networks supporting multinational efforts. These networks form the backbone of what is envisioned to become a global infrastructure that allows the United States to share information rapidly with coalition partners worldwide in support of local, regional, and global combined operations.

The All Partners Access Network is an unclassified (with addresses that do not end in .mil) network that provides interoperability and connectivity among partners over a common platform. The network fosters information exchange and collaboration between Department of Defense and any external country, organization, agency, or individual that does not have ready access to traditional Department of Defense systems and networks.

Requirements Determination

The IMO does not own any processes or procedures of the personnel he supports; rather, he improves staff and MAGTF process efficiencies. Timely quality information promotes a commander's situational awareness and enables informed decisions. In order to define information processes, organizations must first define the information's producers and consumers, the products they produce and consume, the timetable on which consumers need products, and the means by which the product is conveyed and delivered.

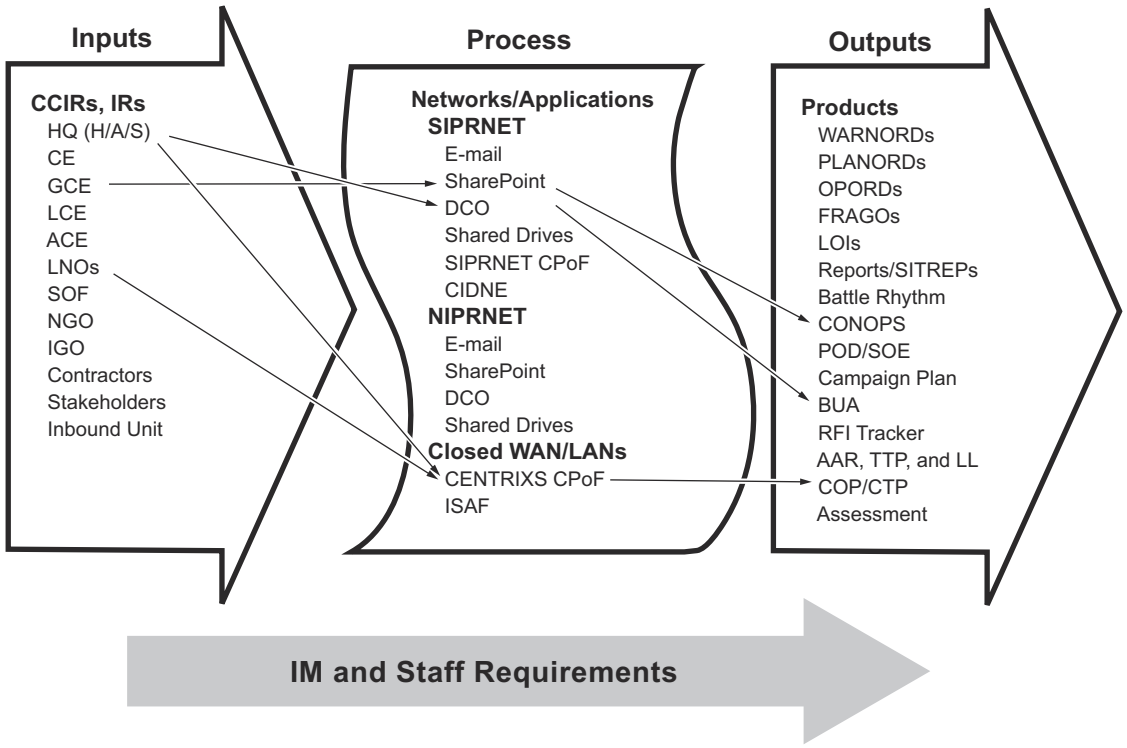
The combination of producer, consumer, and information products are represented as IERs.

Aggregated IERs impact C2 system effectiveness and, thereby, the people who produce/provide the information. Figure 4-1 depicts a generic process for determining IERs, which are the products that are developed, exchanged, and coordinated between producer and consumer. Information exchange requirements drive network, system, and application requirements that must be planned and coordinated to achieve effective organizational command and control and collaboration.

Process Flow

The first step in developing information requirements is to identify discrete information exchanges or requirements supporting a particular task or function. A process flow diagram identifies the series of tasks necessary to support a particular task or function.

Figure 4-2 is an example of a completed process flow diagram. This example delineates the tasks required to provide the information to support the



LEGEND

AAR	after action review/report
ACE	aviation combat element
BUA	Battle Update/Assessment
CCIR	commander's critical information requirement
CE	command element
CIDNE	Combined Information Data Network Exchange
CONOPS	concept of operations
CPoF	Command Post of the Future
DCO	Defense Connect Online
GCE	ground combat element
PLANORD	planning order
H/A/S	higher, adjacent, subordinate
HQ	headquarters
IGO	intergovernmental organization
IR	intelligence requirement
ISAF	international security assistance force
LAN	local area network
LCE	logistics combat element
LL	lessons learned
LNO	liaison officer
LOI	letter of instruction
NGO	nongovernmental organization
POD	plan of the day
SITREP	situation report
SOE	Sequence of Events
SOF	special operations forces
WAN	wide-area network
WARNORD	warning order

Figure 4-1. Example of Information Exchange Requirements.

"collect intelligence" function. Overlaid on the process flow is a depiction of the organizations within a MAGTF responsible for the appropriate components of the process flow.

Configuration Flow

Once the process flow diagrams have been created, the next step is to develop a configuration flow diagram. A configuration flow diagram describes the process flow of systems needed to support specific tasks. A configuration flow diagram is established by performing two steps: determine the system required to perform each task identified by the process flow diagram and identify the network infrastructure necessary to disseminate information produced by personnel performing each task identified by the process flow diagram.

Figure 4-3, on page 4-8, depicts a configuration flow diagram to support the process flow described by figure 4-2. Each system is placed in the appropriate command element organization linked by the proper network infrastructure. Current command relationships and task organization of forces are considered to deve-lop the configuration flow diagram. This methodology permits a command to identify system and network shortfalls or potential vulnerabilities.

Personnel Requirements

In the final step of developing an IM structure, the command identifies personnel requirements from the configuration flow diagram, which determines the number of personnel, skill sets (training), and procedures necessary to support each warfighting function. These requirements are then measured against what is currently being used by the command. This action enables the command to clearly identify deficiencies and implement corrective action. The result is an efficient flow of information within the command IM structure and improved decisionmaking. Figure 4-4, on page 4-9, demonstrates a personnel requirements diagram to support the configuration flow diagram described by figure 4-3.

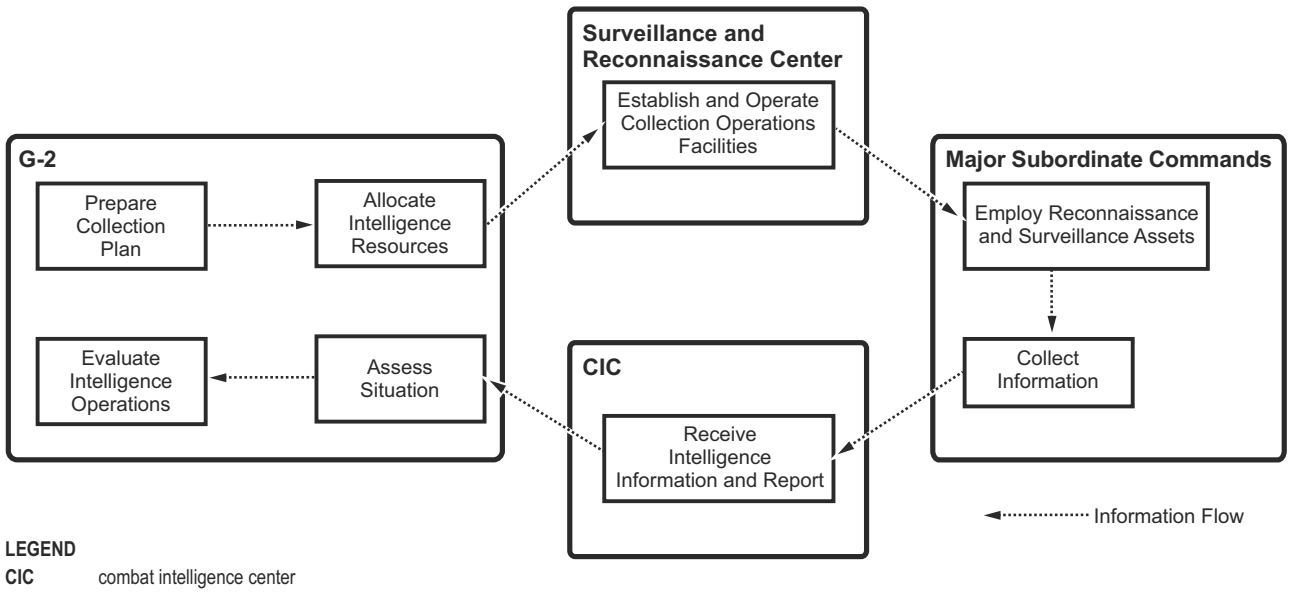


Figure 4-2. Process Flow for Collecting Intelligence.

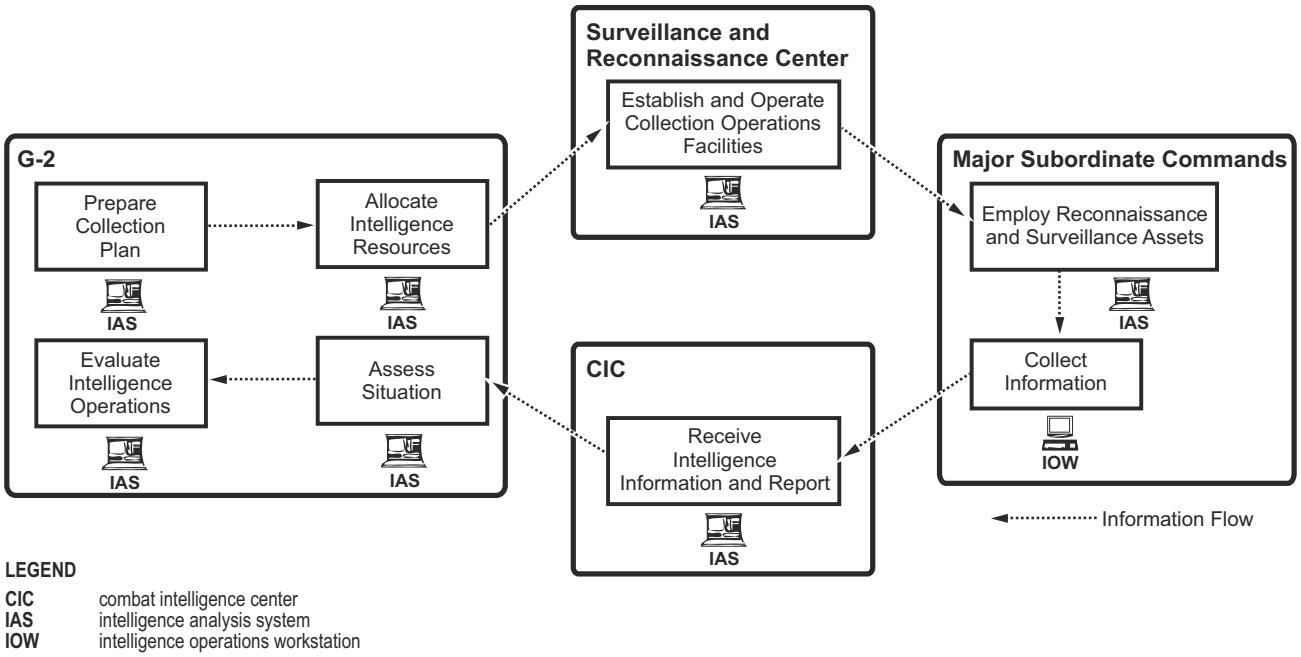


Figure 4-3. Configuration Flow for Collecting Intelligence.

Information Management Documentation, Products, and Tools

Reports Matrix

The reports matrix is a chart of reports provided by subordinate and higher entities in order to coordinate a flow of predictable information for both routine and immediate notification. There is no doctrinal format for the reports matrix, but it should include the time the report is due, period of time covered, priority, classification, recipient, author, format, means of transmission, and comments/requests/recommendations. Reports require a coordinated rhythm as senior headquarters collate subordinate information in reports to HHQ. As reports move through the command structure, information is confirmed and fused for verification/validation. An effective reports matrix is a powerful planning tool to support execution, verify information, and correct the source of information flow problems. A carefully designed reports matrix significantly enhances the efficiency and effectiveness of staffs and decisionmakers.

Battle Rhythm

The battle rhythm (see app. A) is a schedule of key daily events that involve the commander, staff, and subordinates. These events can include B2C2WGs, staff briefings, updates, and visits. The purpose of the battle rhythm is to frame the organizational schedule and facilitate the integration of various events. The C/S or XO is responsible for the battle rhythm, but often delegates the responsibility to IMOs who publish and disseminate the battle rhythm. Commanders and staff officers are responsible for identifying events to be placed on the battle rhythm. The battle rhythm is often the backbone of staff and subordinate coordination and decisionmaking. There is no doctrinal format for a battle rhythm.

Commander's Critical Information Requirements

A CCIR is an information requirement identified by the commander as being critical to facilitating timely decisionmaking. The two subcategories of CCIRs are priority intelligence requirements and

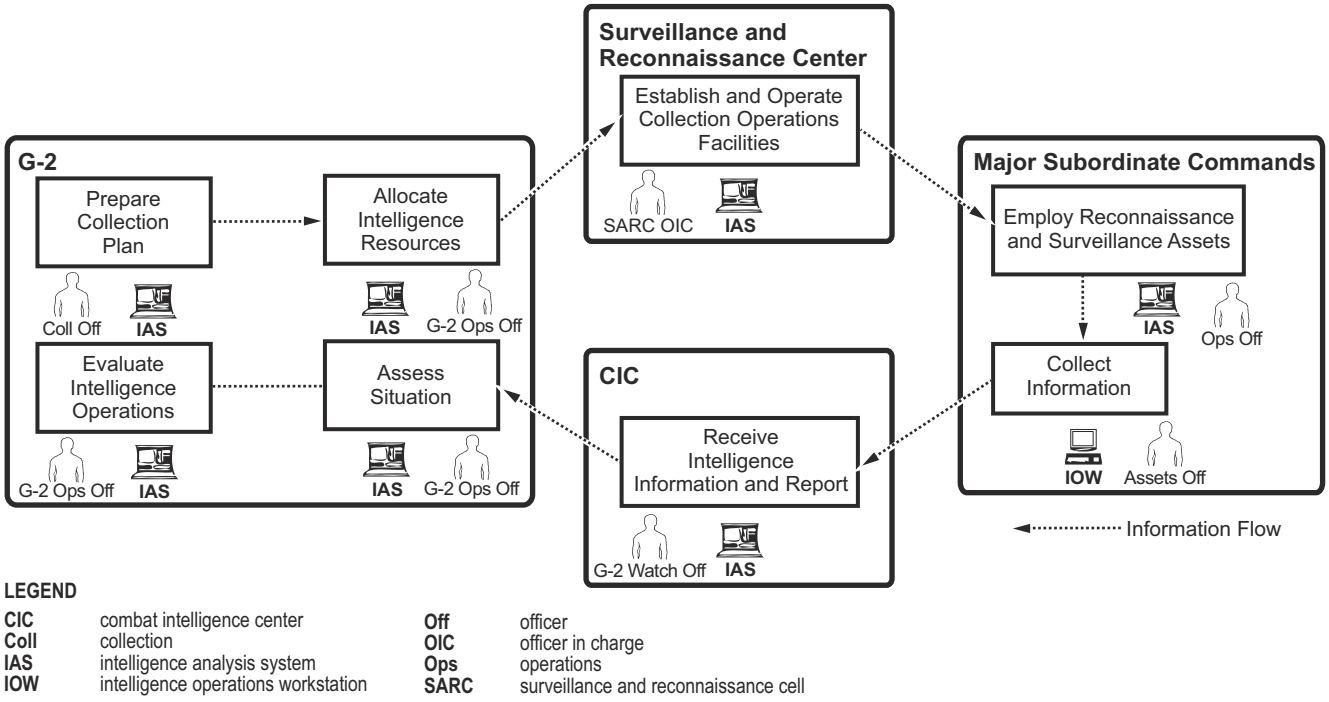


Figure 4-4. Personnel Requirements for Collecting Intelligence.

friendly force information requirements. These information requirements represent the commander's determination of his critical information requirements during each phase of a campaign. Combined with a DSM, CCIRs can focus an organization for relevant response based on strategic opportunity. The requirements can frame information collection and analysis as well as form the basis of response, shaping the battlespace.

The CCIRs are a very important operational framing tool. Instead of reacting to a threat, commanders are able to maintain tempo by controlling the flow of information required to attain the level of understanding they need within the battlespace. Without CCIRs, subordinate units could become overburdened with RFIs; moreover, communication systems and networks could become saturated with requests for nonessential information. As events unfold, the information requirements may change; consequently, new decisions are required and CCIRs must be continuously assessed for relevance to support current and future decisions/situations. The key question is, "What does the commander need to know in a specific situation to make a particular decision in a timely manner?"

The CCIRs have the following functions:

- Reduce the information gaps generated by uncertainties that the commander may have concerning his own force, the adversary, or the environment that he has identified as necessary to maintain situational awareness, plan future activities, and facilitate his ability to make timely decisions.
- Focus the staff on the processed data and knowledge the commander needs for making key decisions (particularly during the course of an operation), reduce information needs and raw data to a manageable set, and ensure that key information requirements are not inadvertently filtered out.
- Define the information required by the commander to better understand the battlespace and to identify risks as well as to make sound, timely decisions in order to retain the initiative.

Decision Support Matrix

The DSM identifies key decision points and actions decided upon by the commander during the preceding planning phase. A DSM can be depicted graphically or in table format to frame an action or operation and to time or vary a response. Decision points are annotated throughout the DSM for commander control of the effort. A DSM can be used at all levels of a command and is a very helpful tool in the planning phase of an operation.

Requests for Information

Requests for information are specific, time-sensitive, ad hoc requirements for information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. The RFIs are generated to answer questions that cannot be resolved with organic assets, and when the information does not exist within internal databases or cannot be satisfied by resident subject matter experts. One RFI process is shown in figure 4-5.

Journals and Logs

Journals and logs represent the chronological record of activity for a unit. For units engaged in contingency operations, the importance of accurate journals and logs cannot be overstated. The unit commander should direct that a command journal be maintained in the operations center and that general staff sections maintain their own journals. The value of accurate journals goes beyond historical analysis and keeps the commander and his staff up to date on significant activities and significant events (SIGEVENTs). These products can be used for analyzing operations, extracting lessons learned, and investigating, when requested.

Information Management Plan and Annex U (Information Management)

The IMP (see app. B) is the expression of the commander's concept for managing and controlling information. The IMP details the planned support of all three elements of command and control—information, people, and C2 infrastructure. The IMP assigns responsibilities and provides instructions for personnel that manage C2 infrastructure. Responsibilities identified by unit standing operating procedure (SOP) do not need to be duplicated in the IMP. Development of an IMP is a vital step of enabling an environment for decisionmakers to receive required information, when needed, in an understandable format. Each command must develop an IMP tailored to manage its information in the context of its mission and current situation or event.

An effective IMP provides guidance to ensure quality information is provided to those who need it in a form they quickly understand. The IMP should cover C2 filtering tools, unique IM personnel needs (duties, responsibilities, and

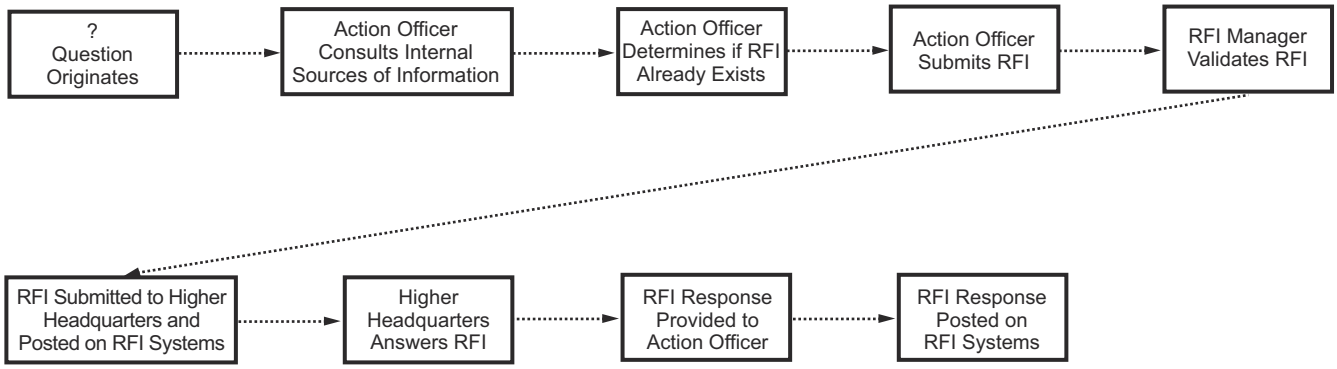


Figure 4-5. Example of a Process Flow Used to Support Request for Information Management.

skill requirements), C2 structure requirements (processes and procedures), and C2 system protection. The IMP should include specific guidance for management of the CTP, CCIR, collaborative planning system, and network applications used to share critical and relevant information. This action may be accomplished through the use of chat rooms, wikis, blogs, Web pages, or other applications.

The development and execution of an effective IMP requires the participation and interaction of all staff sections. The IMP is a collaborative document and each staff section must identify its information requirements, warfighting processes, configuration flow diagrams, and personnel requirements for incorporation into it.

Information management policy and procedures are top-down in nature and the IMP should include considerations for joint and coalition interoperability. Joint task force IM practices will nest within the supported combatant commander's established policies. Likewise, component, MAGTF, and major subordinate commander IM practices must nest within those of the JTF. In fact, commanders and staffs at all levels must have a common understanding of joint IM policy and procedures. See appendix C for the Tri-MEF [Marine expeditionary force] standard IMP format.

Insights and Considerations

The following insights and considerations are lessons learned regarding information management processes and procedures:

- Use CCIRs to prioritize the flow of information. Commander's guidance and CCIRs focus the staff and resources to provide fused information to support decisionmaking. The CCIRs serve as control measures by establishing collecting, processing, analyzing, and disseminating priorities.
- Take charge of knowledge sharing. This is an all-hands responsibility and championed by the commander and senior leaders. It is too important to be left to an individual staff section.
- Delineate authority and responsibility for the different aspects of knowledge sharing, information management, and the associated tools and C2 systems.
- Task the C/S or XO with the responsibility for information management and knowledge sharing, and designate an operationally-focused IMO to report to the C/S or XO.
- Clearly define the headquarters' decisionmaking processes before determining the IM means and tools. Consider both physical and virtual collaboration means to conduct battle rhythm events, which can be physical meetings and phone calls or virtual means, such as secure video teleconferencing, chat rooms, and other collaborative tool suites. Retain the tried and proven use of a scribe to record key information and decisions. Post these summaries on a portal.
- Develop a command climate whereby all personnel are vigilant in protecting sensitive information.
- Identify the communications networks and platforms needed to support the information exchange requirements (e.g., CENTRIXS, SIPRNET, or NIPRNET). Develop processes to share information with interagency and coalition partners not on your communication network.
- Develop an environment that fosters a responsibility-to-share versus a need-to-know mentality with nontraditional partners (e.g., interorganizational and host nation partners) to better support decisionmaking while accounting for the risks associated with compromise on the various networks.
- Develop procedures for RFI management and foreign disclosure within the command. Develop sufficient capacity to enable foreign disclosure and information sharing with partners. This includes ensuring there are foreign disclosure officers and trained foreign disclosure representatives on the staff. Ensure that key information sharing procedures are understood throughout the staff.

- Carefully select tools that are user friendly. Recognize the impact of personnel turnover and training requirements. An adequate IT tool well understood and used by a staff is much more effective than a perfect, continually changing IT tool that is too complex to intuitively understand and use.
- Develop and refine IM processes and procedures through a working group led by the IMO and composed of staff section representatives. The working group reports to an IM decision board, which is chaired by the C/S or XO. Task the working group to maintain currency and relevance of the commander's and staff's knowledge and information assets.
- Disseminate approved IM and knowledge sharing processes through an authoritative IMP. The IMP should define the responsibilities of the IM organization. It should also provide guidance on how to gain and maintain situational awareness; share information; and collaborate with higher, adjacent, and lower organizations throughout the decision cycle. Periodically revise the IMP to reflect improvements to the command's processes as they are developed over time. Be prepared for change. Do not allow an IMP to become stagnant. The IMP must adjust to the individual's decision-making processes.

APPENDIX A
TOOLS, TACTICS, TECHNIQUES, AND PROCEDURES FOR INFORMATION FLOW

This appendix recommends tools and TTP that enhance the efficient flow of relevant information throughout the information hierarchy. The commander's guidance frames parameters for information filters that will be used by the battlestaff to develop and refine useful products. Filtering tools, such as commander's intent, commander's guidance, and CCIRs, enable personnel to enhance information flow and support decisionmaking.

Tools

Commander's Intent

The commander's intent is his personal expression of the purpose of an operation. It must be clear, concise, and easily understood. It may also include how the commander envisions achieving a decision as well as the end state or conditions that, when satisfied, accomplish the purpose. The commander's intent establishes the standards by which success will be judged and sets the tone and framework for effective information management.

Planning Guidance

Commander's guidance is clear, concise guidance that forms the basis for planning. Although not prescriptive in nature, the planning guidance helps the staff make initial judgments on the ways and means to achieve a decision. Based on his personal experience and judgment, the commander articulates clear and concise guidance that helps to focus the IM efforts of the staff and subordinate commanders.

Commander's Critical Information Requirements

The CCIRs are information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintain situational awareness, plan future activities, and facilitate timely decisionmaking. The CCIRs focus the staff on the information the commander needs for critical decisionmaking and reduces information needs to a manageable set. The CCIRs are continuously assessed for relevance to support current and future decisions/ situations. The commander approves CCIRs, but the staff recommends and manages CCIRs to assist the commander.

Tactics, Techniques, and Procedures

The IMOs can use CCIRs to assist in establishing collecting, processing, analyzing, and disseminating priorities.

Information Exchange/Collaboration Tools

To a great extent, the means through which information is exchanged today involves technology. Marines not only have grown reliant on IT to accomplish many objectives, but also have significantly changed TTP as a result of IT. Though the Marine Corps must strive to maximize the efficiencies that IT offers, it must, at the same time, preserve the ability to function and to accomplish its mission without it. The following subparagraphs discuss some of the IT tools commonly used.

E-Mail

A collaboration tool, e-mail facilitates the dissemination of a large amount of information to a large audience. Though e-mail is an effective means of communication, Marines must remember that the human aspects of communication, such as force of personality and tone of voice, cannot be conveyed accurately in an e-mail message. E-mail should

not, if practical, be the sole method of conveying critical or important messages.

Computer Networks

The unclassified government computer network that provides connectivity throughout Department of Defense is the NIPRNET. This network is intended for unclassified official use only and is accessible to all authenticated and authorized users via the Internet. The equivalent network operating at the secret level is SIPRNET. The NIPRNET and SIPRNET are mutually exclusive.

Public and Shared Drives

Due to the nature of the shared resources, all data posted to public and shared drives should be backed up elsewhere as a precaution.

Public folders can contain calendars, message traffic, e-mail, and even some data files, such as documents or spreadsheets. They can store large amounts of information; however, they are somewhat limited in terms of accessibility. Should the need to share information with users outside of the command arise, other applications, such as Web portals or file transfer protocol sites, should be considered.

Commands maintain *shared drives* for the storage and dissemination of information. Shared drives are useful vehicles for making important information available to a large audience. Information stored on shared drives should be current and relevant. Employing the shared drive as a bulletin board, coupled with e-mail notification to relevant users is an efficient use of this resource. For example, a Marine can e-mail users a link to the location of documents on the shared drive without sending an attachment.

In order to ensure a seamless flow of quality information, the following procedures and standards for the shared drive usage have been developed:

- *File folders*. Folders on the shared drive can be organized around the warfighting functions and traditional staff sections.
- *File naming convention*. Documents placed on the shared drive will use a standard file naming convention as detailed in the unit's SOP.
- *Permissions*. Carefully consider how permissions are managed. Who can add, edit, and delete files and folders?

Web Services

Another resource supported by both the NIPRNET and SIPRNET is the ability to maintain Web sites. Like a shared drive, a Web site is an excellent tool for disseminating information. Unlike a shared drive, its functionality lends itself to regular use by even the most inexperienced users and it extends to anyone with a network connection.

A command intranet Web site is a useful means of sharing information and knowledge. It works well in both garrison and tactical environments; although, consideration needs to be given to the lowest unit capable of accessing tactical Web sites in tactical environments. There are several Web portal applications available for use. Some thematic areas that can be addressed on a Web portal are document libraries and Web site procedures.

Document libraries are much like a file server or shared drive, but are made available in a Web site. The IMO needs to consider publishing file naming conventions and file access/upload rules and permissions.

In order to ensure a seamless flow of information, the following procedures and standards for Web site employment have been developed for consideration:

- *Document library*. All section documents will be maintained in the unit document library. Folders on the portal will be organized around the warfighting functions and traditional staff sections. The document library maintains the same look as the shared drive.
- *File naming convention*. Documents placed on an organization's portal shall follow the format developed by the IMO and approved by the commander.

- *Permissions*. Assign appropriate permissions. Consider administration, read and write, and read-only permissions. Typical groups for permission assignment include administrators, section administrators, Web developers, primary staff, internal users, and external users.
- *Calendar*. The operations section will maintain the unit calendar. The unit calendar will only include items of interest at the command level. Unit sections will maintain their own section's calendars with information unique to their section's requirements. Information for the unit calendar will be inputted by section heads/chiefs or forwarded to the operations chief for inclusion into the calendar.
- *News and discussion items*. Relevant information regarding any of the warfighting functions, or unit objectives can be posted here as well as information and discussion items pertaining to the unit and the Marine Corps.
- *Really simple syndication feeds*. Really simple syndication (RSS) feeds are a family of Web feed formats used to publish frequently updated information on Web sites, such as blog entries, news headlines, messages, and video, in a standardized format. The RSS feeds are viewed using an RSS reader, which can be Web based, desktop based or mobile device based. The user subscribes to a particular feed and the RSS reader provides a user interface to view the content. The RSS reader will regularly check the subscription's content to provide updaters at a prescribed interval.
- *Document workspaces.* Document workspaces are great areas for organizing and controlling information regarding specific projects. Document workspaces will be used for the following reasons:
  - For coordination with internal and external agencies on specific documents, such as SOP updates and rewrites.
  - For extranet document approval workspaces to prepare documents to be posted on the extranet.

Best Practices

Daily Battle Rhythm

The daily battle rhythm is the tool used by the commander and his staff to synchronize the daily operating tempo within the planning, decision, execution, and assessment cycle.

Tactics, Techniques, and Procedures

The MAGTF battle rhythm should be posted to the Web site as early as possible in an operation/exercise and changes to the daily schedule should be kept to a minimum. Names for B2C2WGs should be consistent and the battle rhythm should not only reflect synchronization of events across the MAGTF, but should also be nested with the HHQ.

Planning and operating cycles that influence battle rhythm in a MAGTF include intelligence collection, targeting, air tasking orders, reconnaissance tasking, and battle damage assessment collection. The daily battle rhythm should be displayed in the COC.

Web Sites

Web sites are useful for sharing information with a wide audience. The IMP must provide guidance to staff sections and subordinate commands on their responsibilities for establishing and maintaining Web sites throughout the MAGTF. Usually the IMO will have a Webmaster in direct support. The content managers and the IMO should adhere to the following:

- Personally cite and release changes to the OPORD and fragmentary orders (FRAGOs) before they are posted to the Web site, and then personally notify higher, adjacent, and supporting commands after those products are uploaded. Avoid the tendency to "post and forget" when adding critical information to the Web site.
- Have backup plan to transmit OPORD changes and FRAGO(s) in case of Web site failure.
- Frequently check the MAGTF Web site for content and accuracy. This action can be delegated to COC team members and rotated among watch standers.

- Frequently check the MAGTF Web site to guard against public disclosure of personally identifiable information or other sensitive information.
- Ensure critical information, such as FRAGOs, warning orders, CCIRs, or boundary changes, are easily accessed and appropriately flagged for attention on the Web site. Critical information should be consistently grouped in one area.
- Have a means of reporting Web site errors to the COC so that corrective action may be taken in a timely manner.
- Ensure FRAGOs are promptly posted on the Web site with a mechanism that allows the MSC/element to confirm receipt.

Tactics, Techniques, and Procedures

The MAGTF Web site should be simple in design and allow users easy access to critical information. Navigation links should be clearly visible and understandable on the main Web page. Main Web site topics, such as battle rhythm, FRAGO(s), or OPORD, should be prioritized in clearly visible links for rapid access. The MSC Web pages should emulate the main Web page format of the MAGTF command element. This will facilitate Web searches throughout the MAGTF. A good practice is to establish the "three-click rule," which means to design the main Web page so that critical information is no more than three mouse clicks from the main page.

Command Journal

The command journal is a chronological record of events pertaining to a unit or staff section during a given period. All administrative and operational items that have a bearing on the tactics, techniques, operational capabilities, plans, doctrine, and methodology are entered in the command journal. The MAGTF headquarters and each of its MSC headquarters maintains its own command journal.

The SWO must ensure the command journal is being maintained throughout the watch. The journal clerk carries out this task under the immediate supervision of the COC operations chief. The SWO should periodically check the accuracy of the journal. He should also give guidance on the content and timeliness of command journal entries.

The command journal records SIGEVENTs and actions taken by the SWO and the COC team. This enables the later reconstruction of events with minimal friction. The journal also serves as a record for training matters, operational reviews, and historical research. A MAGTF command journal is normally kept (and frequently backed up) electronically and must be available on the Web site. A backup paper copy should also be kept and updated frequently in case of COC power failure.

Tactics, Techniques, and Procedures

The COC should maintain a SIGEVENTs log in close proximity to other key COC electronic displays. A SIGEVENT may be linked to a CCIR, priority intelligence requirement, friendly force information requirement, or a decision point during current operations. Visitors to the COC can refer to the SIGEVENTs log rather than request information from the SWO. The SIGEVENTs log should be posted on the unit Web site for easy reference.

Combat Operations Center Information Displays

The COC electronic information displays help COC watch standers to stay oriented on the current tactical situation as they perform their duties. There are many displays to keep track of during an operation: they can be on laptop or desktop computers or prominently arrayed around the COC floor on large projection screens. Digital, large-screen displays are particularly useful when the SWO wants to draw the attention of watch standers to key events as they unfold. Also, displays allow the commander and battlestaff to visit the COC and get an overall situation update without forcing the SWO to stop his current task and conduct a formal briefing. Some computer applications can zoom the display from a large scale map of the area of operations down to a detailed photo of an area of interest. Unmanned aircraft, aided by tactical data link technology, have enabled real time video display of battlefield areas in the COC. Typical displays found in a COC follow:

- *Common tactical picture.* The CTP is a dynamic graphical representation of all active

elements in the battlespace and all products of those elements within the given area of operations. The CTP is an excellent situational awareness tool for the force commander and thus can be a key element of his decision-making process.

- *Mission/commander's intent/CCIR(s)*. A prominent display of this information in the COC reminds COC personnel of how to focus their efforts to keep the commander informed.
- *Current operations status boards*. The following items are a sample of topics commonly on display in a MAGTF COC, either electronically or in hard copy:
  - Current day of the operation (e.g., D+11/Saturday, 11 Feb 20XX).
  - Phase of the operation (e.g., Phase IIIC, Stage II).
  - Mission-oriented protective posture level (e.g., Level II).
  - Air defense warning condition (e.g., red).
  - Weapons control status (e.g., tight).
  - Threat condition (e.g., ALPHA, BRAVO, etc.).
  - Ground watch (combat power assessment).
  - Intelligence watch (enemy combat power assessment).
  - Logistics (main supply route status).
  - Communications (system status).
- *Command journal*. The COC team should post a SIGEVENTs log (or list) or the actual command journal electronically where the commander and battlestaff can review them periodically without interrupting watch standers.
- *Control measures and targeting display*. A digital electronic display of control/coordination measures serves as a rapid reference in the COC for all watch standers. Advanced Field Artillery Tactical Data System targeting data may also be displayed in order to track significant targets.
- *Unmanned aircraft system video feed*. Unmanned aircraft systems enable real time or near real time displays of the battlefield and are particularly useful during battle drills where decisionmaking is expedited by personal observation of the situation.

Chat

Many users will monitor and use electronic chat rooms during the watch. The best way to manage chat information is to ensure the COC team and subordinate commands adhere to a command chat SOP. This SOP, at a minimum, should offer guidance on the following topics:

- Chat guard chart (e.g., Tac [Tactical] 1, fires, air, logistics).
- Rules for entering and exiting chat rooms.
- Language protocol (e.g., brevity codes, acknowledging orders, flagging critical information).
- Information on the number and type of chat rooms authorized in the MAGTF (chat architecture).
- Rules for the use of "whisper mode" in chat rooms.
- Protocol for date and time stamping entries.
- Rules for setting tools to flag key words, such as troops in contact, mass casualties, weapons of mass destruction, and chemical attack, within the chat software application (not all applications have this capability).
- Rules for "coffee break" events, which are key terms to indicate the watch officer is away from the computer terminal.
- Rules for backing up historical chat records.
- Procedures in the event of chat failure, including alternate means of communication.

Briefing Templates

Preparing for and giving briefings will consume a significant portion of the COC team's time. The exact amount of time spent will vary with each commander and with how much time the COC team spent preparing briefing templates prior to the operation. Rather than prepare each brief from scratch, a prudent watch officer should prepare "briefing shells" tailored to each type of brief he is likely to give. Some briefings, common to every operation, are listed below:

- COC shift change.
- Commander's update.

- Operations/intelligence update.
- HHQ update.

Tactics, Techniques, and Procedures

When preparing briefs, use C2PC [Command and Control Personal Computer] maps and cut and paste them into Microsoft PowerPoint slides. Hide slides that have no change from previous briefs. Limit slide content to three or four key points.

Decision Support Matrix/Decision Support Template

Both of these tools may be displayed individually or together. The DSM identifies key decision points and actions decided upon by the commander during the planning phase. The decision support template is a graphic depiction of the DSM information in C2PC. The electronic display of both tools in the COC gives each COC team member a common reference for situational awareness.

Digital Rules of Protocol

The following subparagraphs describe recommended procedures to ensure the proper use and to promote the proper etiquette when working with collaboration tools and other digital information systems.

Video Teleconferencing

A communication technology that allows collaboration between users at two or more different locations by creating a face-to-face meeting environment. The 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. 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. The systems administrator provides technical assistance as required and the note taker keeps track of taskings, recommendations, and questions, copying questions posted into the minutes at the conclusion of the session and posting the minutes as directed.

Audience members log in at least 10 minutes prior to start time, checking in (voice and chat) with the deputy. If a member attends as a generic sign on (e.g., Planner 22), then a specific identification should be immediately placed in the chat. Audience members should do the following upon entering the chat:

- Choose a seat in a row to facilitate chat in an interest group.
- Change rows to coordinate with other groups.
- Ask questions focused on meeting issues.
- Use private chats to increase collaboration.

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. The following are functions within a chat that users may choose:

- Invite: invites addressee to join the room.
- Join: transports user to the room of the person selected.
- Send note: sends a text message.
- Chat*:* opens a private chat window.
- E-mail: sends an e-mail through the mail system.

Document File Naming Convention

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

- Arabic numerals only (no Roman numerals).
- No spaces. Use an underscore in lieu of a space.
- All documents will use military date (yyyymmdd), then an underscore, then the document's name, then an underscore and the version number (e.g., 20090122_ReportsMatrix_v1.doc).

File Management/Information Storage

Fundamental to the process of information management is the implementation of an information storage system and procedures that provide the ability to store information in a searchable database. The following technologies provide a solid foundation for any command's IM scheme.

The IMO, in conjunction with the G-6, will determine and publish the rules for file and folder naming conventions. Folders can be created along warfighting functions, staff sections/departments, or command lines.

Web portals, both extranet and intranet, should be used as a knowledge repository. Information must be kept current and relevant. Public folders can be shared with members outside of the command as long as they have common access card/public key infrastructure access.

A shared drive should be used to store information as a backup to Web portals. Information must be kept current and relevant on shared drives. Shared drives are typically not accessible to personnel outside of a command and therefore do not serve as a good means of sharing information with them.

File Management/Information Storage Recommendations

Files should be saved to the designated drive of a personal computer or an approved file server or device. Nothing will be saved to the designated primary drive; rather, to a 'home' or personal drive until shared with all. All file naming conventions should be followed as published by the IMO and the file name of a document should not be changed after it has been published to the user community.

Briefing Slide Show File Production and Management

Formal briefing slides should follow a consistent format, so the IMO should make a blank presentation template available for all to use. The following is an example for formatting standards:

- Keep text slides basic, removing logos and only using pictures when required. If graphics are necessary, the image concerned must be grouped and then saved as a .gif [graphics interchange format] or .jpg [Joint Photographic Experts Group] file and then placed on a blank slide.
- Keep briefs short (fewer than 15 slides is ideal). If a longer brief is required, break it into sections with question/clarification breaks.
- Use Arial font for the text. The title should be 36 point type (32 point if two lines), subtitle 28 point, first level 28 point, second level 24 point, third level 20 point, and footers 14 point.
- Make text emphasis bold, underline, and/or italics, limiting the use of colors to when required and only using colors that stand out well.
- Keep text spacing (tool bar, format, line spacing) minimums—lines 0.90, returns 0.25.
- Organize the footer as follows:
  - Lower right: slide number.
  - Lower left: date-time group of briefing and version.
  - Bottom center: point of contact info and JTF portal posting location.

Calendar Operations

Calendar functions will be used to conduct a number of operations in scheduling and management of collaborations. The common use calendar will be maintained for the purpose of coordinating all staff collaborations. Groups, such as plans, operations, or intelligence, 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 main calendar, such that the main calendar shows all entries. All boards, centers, and cells will be 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 meeting 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.

Guidelines for Electronic Mail

E-mail should not be used 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.

E-mail should not be used to disparage others. It is an effective medium for conveying information; however, it is totally inappropriate to use e-mail to disparage or "flame" others. Be aware: no e-mail is private. Keep in mind that any e-mail sent to others becomes part of the public record. Do not send e-mail to individuals unless you wouldn't mind that e-mail being seen by either the JTF commander or public media. Further, BCC [blind courtesy copy] should be limited.

E-mail should be limited to what is essential to the mission. Jokes, stories, and nonessential AVI [Audio Video Interleave] or .jpg files may temporarily improve morale; however, they tend to clutter the local communication infrastructure.

APPENDIX B
INFORMATION MANAGEMENT PLAN

An IMP is developed as part of a tactical or garrison SOP and is similar in nature to Annex U (Information Management) with the exception that annex U is the IMP of a named OPORD or plan.

This appendix provides an example of one format of an IMP that can be configured for use by any specified size of command.

UNIT HEADING

IN REPLY REFER TO:
SSIC
IMO
1 Nov XX

UNIT ORDER XXXX.XXX

From: Commanding Officer

To: Distribution

Subj: UNIT INFORMATION MANAGEMENT PLAN

Ref: (a) MCWP 3-40.2, *Information Management*.

(b) MCDP 6, *Command and Control*.

Encl: (1) Staff Section Mission Essential Tasks.

(2) Staff Section Information Requirements.

(3) Plan of Action and Milestones.

(4) Systems Usage and Training Requirements.

1. Purpose. This order provides planning guidance and direction to all staff sections with regard to execution of the IMP. Per the references, the unit will develop and execute an IMP that will capture how the command manages and controls information.

2. Scope. This order constitutes the primary planning document for the IMP. It describes the purpose and objectives of the IMP, identifies all major participants, identifies the IMP framework, assigns tasks associated with the execution of the IMP, and provides general information regarding the execution of the IMP.

3. Information Management Plan

a. The IMP will aid the unit in training and maintaining a common information environment through the predeployment training program, deployment, and postdeployment period. The end state of the IMP is to meet the unit commander's IM vision statement:

The UNIT IM plan will increase the effectiveness of the command's decision cycle by creating an information environment that links operational and administrative information together using existing systems and tools. With the IM board oversight, the plan will: (1) develop an operational information architecture; (2) identify internal and external information exchange requirements; and (3) identify training shortfalls in order to provide timely, analyzed, relevant information to the commander that enhances his decisionmaking process.

b. Information Management Plan Objectives.

(1) Create a culture of a "matter of practice."

(2) Identify information requirements.

(3) Streamline the flow of information by developing a process and procedures.

(4) Eliminate unnecessary information.

(5) Develop an information environment that is not additive in nature.

c. Ways in which the unit communicates.

(1) OPORDs.

(2) FRAGOs.

(3) CCIRs.

(4) Situation reports.

(5) Letters of instruction.

(6) Classified and unclassified message traffic.

(7) SIPRNET chat.

(8) SIPRNET e-mail.

(9) NIPRNET e-mail.

(10) Sensitive compartmented information networks.

(11) Web pages.

(12) Secure and nonsecure voice products.

(13) Papers.

(14) Briefs.

4. Concept of Operations. The IMP framework is a six-step program.

a. Step 1: Identify Mission-Essential Task List. The identification of section mission-essential task lists (METLs) will allow the staff to identify those areas that require further analysis in order to capture required processes and information requirements.

b. Step 2: Identify Staff Section Information Requirements. Section information requirements are derived by performing mission analysis of a section's METLs. An information requirement can be answered via either a process or a system.

c. Step 3: Identify Process/System Improvement. The process is defined as those actions performed that require inputs and outputs to answer an identified information requirement. Once all information requirements have been identified, staff sections and the IM board will validate and prioritize current processes/systems and assess whether improvements can be applied. Improvements can be in the form of a process modification, training solution, personnel augmentation, or use of a system/technology.

d. Step 4: Identify Training Requirements. Training is a fundamental component of the IMP. The information requirements identified will be the base of the IMP training matrix. The IM board will also look at the commercial sector for innovative training opportunities.

e. Step 5: Identify IM Gaps. To identify IM gaps, the staff sections will need to review their METLs and information requirements and identify those information requirements they have not been able to answer. Once an IM gap is identified, the IM board will determine if the gap can be filled with a resource internal to the command. If the gap cannot be answered internal to the command, the IMO will coordinate with outside agencies to assess potential solutions.

f. Step 6: Begin Training. Training is a continuous process.

5. Tasks

a. Information Management Officer

(1) Publish the IMP.

(2) Coordinate training scheduling with S-3, Marine Corps resources, required civilian organizations, and sections.

(3) Schedule and chair IM board meetings to discuss progress of predeployment IMP.

(4) Track progress of IMP execution.

b. S-3 Officer (Operations)

(1) Provide a staff noncommissioned officer to serve as IM chief.

(2) Serve as the co-chair of the IM board.

(3) Ensure IM training events are added to the training, exercise, and evaluation plan.

c. S-4 Officer (Logistics). Coordinate fiscal requirements in relation to civilian IM training requirements.

d. S-6 Officer (Communications System)

(1) Serve as the assistant IMO and co-chair of the IM board.

(2) Coordinate with the IMO in the establishment of an IMP.

(3) Provide communication estimates of supportability for IM requirements identified by the IM board.

e. Information Management Chief

(1) Serve as Webmaster.

(2) Coordinate Web external support.

(3) Assist the IMO and assistant IMO.

(4) Supervise the information support coordinators.

f. All Staff Sections and Special Staff

(1) Develop section IERs.

(2) Provide an officer or staff noncommissioned officer to serve as IM board representative.

(3) Identify in writing a section information support coordinator.

(4) Identify system and process training requirements.

(5) Identify specific training requirements for section-specific information requirements.

(6) Coordinate specific training for sections with the appropriate training resource.

6. Coordinating Instructions

a. Ensure that appropriate personnel attend required training.

b. Provide personnel to attend IM board meetings.

c. Coordinate with functional system representatives to identify support requirements and resource availability.

7. Administration and Logistics. Omitted.

8. Command and Signal. Omitted.

I.M. IN CHARGE

Staff Section Mission-Essential Tasks

The mission-essential task areas in table B-1 are examples of how staff sections are responsible to produce or manage information products.

Table B-1. Example Mission-Essential Task Checklist.

Section	Mission-Essential Task
S-1 (Administration)	Provide personnel accountability
	Conduct personnel administration
	Manage the command's personnel casualty report
S-2 (Intelligence)	Provide intelligence updates as required in order to reduce uncertainty and provide for force protection
	Track and manage security clearances and isolated personnel reports
	Track, manage, and maintain updated intelligence-specific classified document and geospatial information and services holdings
	Provide timely intelligence support for all mission types
S-3 (Operations)	Plan, coordinate, and execute all operations and exercises
	Plan, coordinate, and document command element training
	Manage and execute the rapid response planning process and deliberate planning process
	Conduct coordination, planning, training, and execution of all fires
	Conduct planning and coordination of aviation in support of exercises and operations
	Provide and maintain and operations center capable of planning, executing, and coordinating with higher, adjacent, and subordinate units
	Conduct training and develop, maintain, and disseminate a COP
	Provide operational support to the forward command element
	Provide combat camera assets for documentation of training and operations
	Compile and disseminate operational reporting and commander's brief
	Provide a MAGTF Assessment and Consequence Management Set
	Provide detection/identification/decontamination package
	Provide accurate readiness status report
	Develop, coordinate, and manage time-phased force deployment data
	Develop, coordinate, and manage the ammunition allocation plan
	Manage and maintain the unit historian program
	Manage and maintain a safety awareness program
	Provide, develop, and implement a force protection plan

Table B-1. Example Mission-Essential Task Checklist (continued).

Section	Mission-Essential Task
S-4 (Logistics)	Plan and coordinate internal and external combat service support
	Prepare logistic/combat service support plans, orders, letters of instruction
	Provide contracting support
	Manage budget
	Manage supply warehouse
	Manage hazardous waste/hazardous materials program
	Provide armory support to command element
	Provide precision weapons armorer support
	Prepare load plans
	Identify and validate lift requirements
	Manage ammunition account
	Manage ground equipment readiness
S-6 (Communications)	Conduct communications planning, engineering, and supervision for assigned Marine Corps and other Service communications elements
	Plan, install, and operate wideband data and voice services
	Plan, install, and operate single-channel radio circuits
	Develop communication plans and orders
	Coordinate support to higher, adjacent, and subordinate command communications system requirements
	Support communication requirement to command and control nodes
	Exercise management of the tactical network
	Publish communication-electronic operating instructions
	Provide communication support to the forward command element
	Provide secure data and voice capability for liaison elements
	Provide Global Broadcast Service
	Provide electronic management key system support
	Protect information systems
Staff Judge Advocate	Provide command legal advice to the commander regarding international law, military justice, and fiscal and administrative law
	Advise commander and staff on legal issues related to release of information
	Assist command with conduct, processing, and storage of investigations
	Advise commander on the law of war and rules of engagement
	Train personnel on the law of war and rules of engagement
	Investigate and process foreign claims
	Provide legal assistance to eligible personnel
Medical	Provide force health protection
	Provide health service support
	Support casualty evacuation

Table B-1. Example Mission-Essential Task Checklist (continued).

Section	Mission-Essential Task
Public Affairs	Produce articles, imagery, radio, and video broadcasts of training and operations for release
	Develop and execute External Media Information Plan
	Develop and execute Public Affairs Crisis Communications Plan
	Develop and execute Community Relations Plan
	Develop and execute Internal Information Plan
	Conduct unit media training
	Maintain unit public Web site
	Research, develop, disseminate, and update public affairs guidance
	Manage unit Hometown News Release Program
	Develop and execute Annex F (Public Affairs) of the OPORD
	Produce, sell, and contract the printing of the unit cruise book
	Monitor internal and external media outlets for current trends in public perception of military affairs
Chaplain	Coordinate religious ministry services
	Manage American Red Cross message handling
	Coordinate and manage special programs
	Affect suicide prevention
	Act as advisor for family readiness

Staff Section Information Requirements Table

Section information requirements are derived by performing mission analysis of a section's METLs and would be filled out for each section in such a table as shown in table B-2.

Table B-2. Staff Section Information Requirements Table.

Information Requirement	Action	Process (Inputs / Outputs)	System

Systems Usage and Training Requirements

Table B-3 is an example of a matrix that describes the systems usage and training requirements for the unit.

Table B-3. Example Systems Usage and Training Requirements Matrix.

SYSTEMS USAGE AND TRAINING REQUIREMENTS													
	S-1	S-2	S-3	S-4	S-6	MEDICAL	SJA	CHAPLAIN	PAO/ COM CAM	HQ CMDT	ACE	GCE	LCE
MS Office	3	3	3	3	3	3	3	3	3	3			
MS Project	3	3	3	3	3	3	3	3	3	3			
Website	3	3	3	3	3	3	3	3	3	3			
Chat	1	1	1	1	1	1	1	1	1	1	1	1	1
DMS													
DTS													
CMCC													
Postal													
Awards System													
A-PES													
MOL													
ODSE													
Medical Readiness Reporting System (MRRS)						1							
Electronic Deployment Health Assessment (EDHA)						1							
CLC2S				1								1	1
TCPT				1								1	1
BCS3				1								1	1
MDSSII				1								1	
AALPS				1								1	
C2PC			1	1							1	1	1
CPOF			1	1							1	1	1
FBCB2-BFT			1	1							1	1	1
GCCS												1	
IOS		1	1									1	
AFATDS			1									1	
EMT			1									1	
MARINELINK		1										1	
INTEL ANALYSTS NOTEBOOK		1										1	
PFPS		1										1	
BATS		1										1	
MS Active Directory					1								
MS Exchange					1								
TALON/BGAN					1								
CISCO Networking					1								
REDCOM Switching					1								
ECCS					1								
USMC IA Systems					1								
MSWAN					1								
LEGEND	1 - Training Required												
	2 - Training can be obtained from within the unit												
	3 - Training required from external sources												

APPENDIX C
ANNEX U (INFORMATION MANAGEMENT)

This appendix provides a sample of the agreed-upon Tri-MEF Annex U (Information Manage-ment). This Annex U is focused on supporting a Marine expeditionary force-level MAGTF, but the same principles are applicable for all commands. A unit's IMP will serve as the basis for developing/building an Annex U in support of operations/exercises. Various components of an Annex U will not be indicated because they are referenced in the unit's IMP or tactical (TAC) SOP, while others will be inserted from the IMP or TAC SOP and configured for the specific mission.

CLASSIFICATION

Copy no._____ of_____ copies
ISSUING UNIT
PLACE OF ISSUE
Date/time group
Message reference number

ANNEX U TO XX MARINE EXPEDITIONARY FORCE (XX MEF) OPERATION ORDER 10-01 (U)
(U) Information Management

(U) REFERENCES:

(a) XX MEF Tactical Portal: http://www.xxmef.usmc.smil.mil
(b) TAC SOP, CURRENT OPERATIONS, XX MEF (Annex C)

(U) Time Zone:

1. (U) Situation

a. (U) General. This annex provides guidance on processes and procedures for information management in support of XX MEF. It promulgates concepts, assigns responsibilities, and provides planning guidance for all XX MEF forces and joint or coalition forces operational or tactical control to XX MEF. All IM planning and execution will be in accordance with references (a) through (b) except as noted in this annex.

b. (U) Enemy

(1) (U) See Annex B (Intelligence).

CLASSIFICATION

(2) (U) Forces and nations in the XX MEF area of operations have the capability to:

(a) (U) Employ collection systems and means to record and analyze clear-voice coalition force communications.

(b) (U) Collect, aggregate, analyze, and disseminate information from publicly accessible Web sites, compromised NIPRNET Web sites, and compromised publicly accessible mail servers. The threat to coalition networks continues to be determined in theater by the G-6.

c. (U) Friendly. See Annex A (Task Organization).

(1) (U) Command Relationships. See Annex J (Command Relationships).

(2) (U) Attachments and Detachments. See Annex A (Task Organization).

2. (U) Mission. See base order.

3. (U) Execution

a. (U) Concept of Information Management. The purpose of information management is to provide the commander and his staff accurate, relevant, and timely information in order to effectively command and control forces to accomplish the assigned mission. Many information processes are specific to a warfighting function, but there are many others that are shared across the staffs. In both cases XX MEF will use common IM processes to maximize the information pipeline for increased accuracy, timeliness, and relevancy of information to include our coalition partners. This includes the specific processes and systems governed by IM personnel.

(1) (U) In general, the enduring tasks of the IM architectures, tools, and processes for (MISSION NAME) will continue to provide essential IERs for ongoing operations. These tasks, while decentralized in execution, must be closely coordinated with higher, adjacent, and subordinate units already in place. Additionally, XX MEF will be prepared to geographically transition current bases and/or forward operating base locations and command, control, communications, and computers system support within the area of operations when directed.

(2) (U) Geographic Transition. Any realignment of forces requiring the transition of existing C2 architectures and systems will require planning, coordination, and preparation with XX MEF. Units will exercise the principles of redundancy and the tenets of passing control when geographic transitions are directed. Units may not execute except as directed by HHQ to ensure uninterrupted C2 architecture is maintained at all times.

CLASSIFICATION

b. (U) General Guidance

(1) (U) Tactical Data Networks. Four tactical data networks will be the primary Internet protocol wide-area networks employed during this campaign: SIPRNET, NIPRNET, CSD [Common SIPRNET Domain], and other coalition networks.

(a) (U) SIPRNET. Provides classified connectivity to the SIPRNET down to end users.

(b) (U) NIPRNET. Provides connectivity to NIPRNET and the Internet.

(c) (U) CSD. Provides filtered connectivity via SIPRNET to Secret//Rel USA, AUS, CAN, GBR/.

(d) (U) Other coalition networks as required by the CCDR, which provide connectivity among coalition forces in the theater, including virtually all coalition forces.

(2) (U) Common Operating Picture Management. XX MEF will maintain appropriate command and control nodes for the COP. For information on the COP, see Appendix 2.

(3) (U) XX MEF Portal. XX MEF internal and external portals will be integrated, maintained, and managed by the IMO in concert with XX MEF staff section content managers. A separate site will be used for segregating NOFORN [Not Releasable to Foreign Nationals/Governments/Non-US Citizens] material. See Appendix 5.

(4) (U) Collaborative Systems. These collaborative systems will be managed by the IMO. See Appendix 3.

(5) (U) Software Versioning. XX MEF Tactical Systems Software has been baselined with HHQ and service chains. Changes to the XX MEF baseline are not authorized unless coordinated through the XX MEF IMO. Tactical software includes software fielded with all systems of record as well as critical commercial off-the-shelf software. Software that is currently authorized for limited user evaluations may not be distributed beyond those users without coordination with the XX MEF IMO or authorization from HHQ. New applications will be vetted through the Information Management Working Group and approved by the Information Management Board prior to deployment in XX MEF networks in order to limit the tasks associated with maintaining additional applications that are not part of a program of record. See Appendix 3 for a detailed list of software and versions.

(6) (U) Coalition Information Sharing. In the event a coalition unit is assigned operational/tactical control to XX MEF, the following guidance applies: enabling

CLASSIFICATION

command and control of a subordinate unit from a different nation (higher-to-lower) is a bilateral responsibility; subordinate units should coordinate through an assigned liaison officer for all efforts to enable C2 information sharing.

(a) (U) Responsibilities from a command to an adjacent unit from a different nation are the responsibility of both units. Both commands are responsible for terminating their communications circuits at the other command. Where liaison teams are required, both commands will provide liaison team personnel and appropriate communications systems.

(b) (U) Foreign disclosure officer will approve disclosure or release of applicable information.

(7) (U) Proper Classification of Information, Information Security, and Operational Security.

(a) (U) The baseline classification for classified information is SECRET// REL _ _ _//FOR VIEW BY (coalition partners). Whenever appropriate, using this level of classification provides the widest dissemination to forces within the area of operations. All units must be familiar with changes to the proper classifications of classified material in order to ensure effective information flow among (coalition partners) personnel. Specifically, units should understand the distinction between SECRET; SECRET//REL USA, AUS, CAN, GBR/; and SECRET//REL _ _ _//FOR VIEW BY (coalition partners).

(b) (U) Maximum use will be made of information security and operational security policies and procedures detailed in Annexes K and Y to prevent disclosure of vital information to opposing forces. Message classification software is used by XX MEF to assign appropriate level information classification for email traffic. All units must ensure incident response and reporting capability is established to comply with XX MEF G-6 Cyber Security (CY) policies.

(8) (U) Common Systems and Processes. XX MEF units will maintain commonality of IM processes and systems to the greatest extent possible, balanced by the information requirements of individual commanders, throughout all phases of operations. See Appendix 3.

CLASSIFICATION

c. (U) Tasks and Responsibilities

(1) (U) XX MEF Staff Directorates.

(a) (U) Ensure IMO is assigned (primary or collateral duty) and that he reports the following to the XX MEF IMO: contact information, unique requirements for IM or C2 system technical support for the section, and staff organization. Ensure he coordinates IM-related plans, SOPs, and orders.

(b) (U) Coordinate any external emerging Web or C2 system support requirements with the Science and Technologies section and the IMO.

(2) (U) XX MEF IMO

(a) (U) Develop and publish guidance on IM and staff action processes for the operations and maintenance of the XX MEF COP architecture, the XX MEF portal, the command journal, and other Web-based tools in accordance with reference (b) and as directed by the Commanding General, XX MEF. See Appendix 5.

(b) (U) Provide directive guidance on C2 systems within XX MEF to ensure synchronization and integration for staff and MSCs. See Appendix 3.

(c) (U) Provide guidance on the best methods to exchange data between systems using multiple networks to include SIPRNET, NIPRNET, Common SIPRNET Domain, and other coalition networks.

(d) (U) Provide technical support personnel, including deployed contractors, to support C2 systems and information systems as required.

(e) (U) Establish a Web development section to support XX MEF headquarters and all XX MEF units that require Web-based support services.

(f) (U) Provide XX MEF portals as required.

(g) (U) Review all subordinate supporting IM annexes developed in support of this order.

(h) (U) Conduct Information Management Working Group meetings with the MSC IMOs.

CLASSIFICATION

(3) (U) General Tasks for XX MEF Subordinate Commands. These tasks are directed to ensure rapid integration and continuing interoperability of XX MEF forces.

(a) (U) Install, operate, and maintain C2 systems in accordance with the information presented in this annex.

(b) (U) Assign a unit IMO (as a primary duty for regiment-sized elements or collateral duty for battalions). The unit IMO will report to the XX MEF IMO with contact information; unique requirements for IM or C2 system technical support; unit task organization; and IM plans, SOPs, and orders.

(c) (U) Participate in the IM working group and other scheduled or on-call events published by XX MEF IMO.

(d) (U) Act as functional area manager for those C2 and information systems communities of interest identified in Appendix 3.

(e) (U) Establish and maintain a tactical portal or coordinate for the use of a supported/supporting unit portal per Appendix 5.

(f) (U) Maintain an online Web-based command journal or coordinate for the use of a supported/supporting unit command journal. A command journal will be displayed on each MSC's primary tactical portal (or supported/supporting unit portal).

(4) (U) Specified Tasks

(a) (U) Aviation Combat Element

1 Act as alternate command post.

2 In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

3 BPT [be prepared to] conduct and support C2 system software and hardware upgrades to include units within the task organization.

(b) (U) Logistics Combat Element

1 Serve as an intermediate level node for IM flow and C2 systems architecture.

2 In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

CLASSIFICATION

3 BPT conduct and support C2 system software and hardware upgrades to include units within the task organization.

(c) (U) Ground Combat Element

1 Identify and coordinate any Service-specific requirements necessary to integrate Army Battle Command Systems as required.

2 In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

3 BPT conduct and support C2 system software and hardware upgrades to include unit within your task organization.

(d) (U) Additional MSCs/MSEs

1 In addition to standard C2 architecture, establish and maintain a mid-tier server capability for C2 systems as required.

2 BPT conduct and support C2 system software and hardware upgrades to include units within the task organization.

d. (U) Coordinating Instructions

(1) (U) The Information Management Working Group, which consists of all XX MEF unit IMOs and/or information managers, will convene bi-monthly. Additional sessions may be scheduled as required and will be published via e-mail and in the XX MEF Daily Battle Rhythm. See Ref (b) TAC SOP.

4. (U) Administration and Logistics. Refer to Annexes E and D, respectively.

5. (U) Command and Signal. Units assigned as alternate command posts or in the succession of the chain of command shall maintain the ability to provide C2 system support and information resources to the extent required to carry out succession of command or activation of an alternate command post. Each MSC is responsible for providing its own Continuity of Operations Plan and data recovery capability.

ACKNOWLEDGE RECEIPT

I. A. MARINE
Lieutenant General, USMC
Commanding

Page number

CLASSIFICATION

CLASSIFICATION

APPENDICES:

1–Daily Battle Rhythm Management
2–Common Operating Picture Management
3–Collaborative Systems and Tools
4–C2 Systems
5–Portal Development and Administration
6–Blue Force Situational Awareness

OFFICIAL:

s/
U. R. MARINE
Colonel, USMC
Chief of Staff

GLOSSARY

SECTION I. ACRONYMS

B2C2WG . . . . . board, bureau, center, cell, and working group

C2 . . . . . command and control
C2PC . . . . . command and control personal computer
CCIR . . . . . commander's critical information requirement
CENTRIXS . . . . . Combined Enterprise Regional Information Exchange System
COC . . . . . combat operations center
COP . . . . . common operational picture
C/S . . . . . chief of staff
CTP . . . . . common tactical picture

DSM . . . . . decision support matrix

e-mail . . . . . electronic mail

FRAGO . . . . . fragmentary order

G-2 . . . . . assistant chief of staff, intelligence
G-3 . . . . . assistant chief of staff, operations
G-6 . . . . . assistant chief of staff, communications system

HHQ . . . . . higher headquarters

IAM . . . . . information assurance manager
IER . . . . . information exchange requirement
IM . . . . . information management
IMO . . . . . information management officer
IMP . . . . . information management plan
IT . . . . . information technology

JTF . . . . . joint task force

MAGTF . . . . . Marine air-ground task force
MCDP . . . . . Marine Corps doctrinal publication
MEF . . . . . Marine expeditionary force
METL . . . . . mission-essential task list
MSC . . . . . major subordinate command

NIPRNET . . . . . Nonsecure Internet Protocol Router Network

OPORD . . . . . operation order

RFI . . . . . request for information
RSS . . . . . really simple syndication

S-1 . . . . . personnel officer
S-2 . . . . . intelligence officer
S-3 . . . . . operations officer
S-4 . . . . . logistics officer
S-6 . . . . . communications system officer
SIGEVENT . . . . . significant event
SIPRNET . . . . . SECRET Internet Protocol Router Network
SOP . . . . . standing operating procedure
SWO . . . . . senior watch officer

TAC . . . . . tactical
TTP . . . . . tactics, techniques, and procedures

XO . . . . . executive officer

SECTION II. DEFINITIONS

commander's critical information requirement—An information requirement identified by the commander as being critical to facilitating timely decisionmaking. (JP 1-02) Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. The two subcategories are priority intelligence requirements and friendly force information requirements. Also called **CCIR**. (MCRP 5-12C)

common operational picture—A single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness. Also called **COP**. (JP 1-02)

common tactical picture—An accurate and complete display of relevant tactical data that integrates tactical information from the multitactical data link network, ground network, intelligence network, and sensor networks. Also called **CTP**. (JP 1-02)

information assurance—Actions that protect and defend information systems by ensuring availability, integrity, authentication, confidentiality, and nonrepudiation. Also called **IA**. (JP 1-02)

information filter—A filter used to assess the value of information and discard what is not pertinent or important.

information flow—The movement of information.

information management—The function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals and organizations in a way that optimizes access by all who have a share in that data or a right to that information. (JP 3-0) The sum of the processes for the collaboration and sharing of information. Also called **IM**. (Proposed for inclusion in the next edition of MCRP 5-12C)

information requirements—In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 1-02)

knowledge management—The integration of people and processes, enabled by technology, to facilitate the exchange of operationally relevant information and expertise to increase organizational performance. (Proposed for inclusion in the next edition of MCRP 5-12C)

request for information—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)

situational awareness—Knowledge and understanding of the current situation that promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that fosters an ability to determine quickly the context and relevance of events that are unfolding. (MCRP 5-12C)

REFERENCES AND RELATED PUBLICATIONS

Federal Publications

United States Code, Title 44, *Public Printing and Documents*, chapter 21, "National Archives and Records Administration"

United States Code, Title 44, *Public Printing and Documents*, Administration and chapter 33, "Disposal of Records"

Department of Defense Instruction

O-8530.2 Support to Computer Network Defense (CND)

Chairman of the Joint Chiefs of Staff Instruction (CJCSI)

3151.01B Global Command and Control System Common Operational Picture Reporting Requirements

Joint Publications (JPs)

1 Doctrine for Armed Forces of the United States
1-02 Department of Defense Dictionary of Military and Associated Terms
3-0 Joint Operations
6-0 Joint Communications System

Marine Corps Publications

Marine Corps Doctrinal Publications (MCDPs)
1 Warfighting
1-0 Marine Corps Operations
3 Expeditionary Operations
5 Planning
6 Command and Control

Marine Corps Warfighting Publication (MCWP)
5-1 Marine Corps Planning Process

Marine Corps Reference Publications (MCRP)
5-12C Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms

Marine Corps Orders (MCOs)
5210.11E Marine Corps Records Management Program
5400.52 Department of the Navy Deputy Chief Information Officer Marine Corps Roles and Responsibilities

Department of the Navy

Department of the Navy Knowledge Management Strategy

Miscellaneous

ACE Commander's Primer on Battle Command Displays, dated 15 February 2009

Bennet, Alex & David, 2006. *Defining Knowledge*. Mountain Quest Institute

Marine Corps Information Enterprise (MCIENT) Strategy Neilson, Robert E, (2001). Information Resources Management College, National Defense University. "Knowledge Management and the Role of the CKO," in *Knowledge Management: Catalyst for Electronic Government*, Vienna, Virginia.]