NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

AN ARCHITECTURAL APPROACH TO
STRATEGIC INFORMATION SYSTEMS PLANNING
FOR THE OFFICE OF NAVAL INTELLIGENCE

by

Bruce F. Loveless

September 1994

Principal Advisor: Carl R. Jones
Associate Advisor: James C. Emery

REPORT DOCUMENTATION PAGE			Form approved OMB No. 0704-188

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1994	Master's Thesis

4. TITLE AND SUBTITLE
AN ARCHITECTURAL APPROACH TO STRATEGIC INFORMATION SYSTEMS PLANNING FOR THE OFFICE OF NAVAL INTELLIGENCE (U)

5. FUNDING NUMBERS

6. AUTHOR(S)
Bruce F. Loveless

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Systems Directorate (ONI-7)
Office of Naval Intelligence
4600 Silver Hill Road, Washington, D.C. 20389-5000

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (Maximum 200 words)
Strategic information systems (IS) planning aligns an organization's information systems with its critical strategic goals and supporting mission-specific functions. This thesis demonstrates a structured approach to strategic IS planning and provides a guide for developing an information systems architecture to support the organizational goals of the Office of Naval Intelligence (ONI). By first examining established information systems planning practices, architectural design methodologies, Department of Defense (DoD) guidelines, and published ONI organizational objectives, this thesis guides the reader through the decision-making process involved in strategic IS planning. The methodology is structured on guidance provided by the DoD's Technical Architecture Framework for Information Management (TAFIM) Standards-Based Architecture (SBA) Planning Guide. This thesis demonstrates the validity of using the structured architectural approach, presented by the TAFIM and other strategic IS planning concepts, in concert with intelligence-specific IS planning guidance to systematically address the issues, problems, and critical decisions faced by organizations attempting the strategic IS planning process.

14. SUBJECT TERMS
C2, C4I, IS, IT, IM, ITM, DoD, CIM, C4IFTW, TAFIM, Strategic Planning, Information Technology, Information Systems, Systems Management, Systems Architecture

15. NUMBER OF PAGES
167

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF THIS ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18

Approved for public release; distribution is unlimited.

AN ARCHITECTURAL APPROACH
TO
STRATEGIC INFORMATION SYSTEMS PLANNING
FOR THE
OFFICE OF NAVAL INTELLIGENCE

by

Bruce F. Loveless
Lieutenant, United States Navy
B.S., United States Naval Academy, 1986

Submitted in partial fulfillment of
requirements for the degree of

MASTER OF SCIENCE
IN
INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1994

Author: Bruce F. Loveless

Approved by: Carl R. Jones, Principal Advisor

James C. Emery, Associate Advisor

Reuben T Harris for
David R. Whipple, Chairman,
Department of Systems Management

ABSTRACT

Strategic information systems (IS) planning aligns an organization's information systems with its critical strategic goals and supporting mission-specific functions. This thesis demonstrates a structured approach to strategic IS planning and provides a guide for developing an information systems architecture to support the organizational goals of the Office of Naval Intelligence (ONI). By first examining established information systems planning practices, architectural design methodologies, Department of Defense (DoD) guidelines, and published ONI organizational objectives, this thesis guides the reader through the decision-making process involved in strategic IS planning. The methodology is structured on guidance provided by the DoD's Technical Architecture Framework for Information Management (TAFIM) Standards-Based Architecture (SBA) Planning Guide. This thesis demonstrates the validity of using the structured architectural approach, presented by the TAFIM and other strategic IS planning concepts, in concert with intelligence-specific IS planning guidance to systematically address the issues, problems, and critical decisions faced by organizations attempting the strategic IS planning process.

TABLE OF CONTENTS

I. INTRODUCTION

A. PURPOSE OF THESIS

The purpose of this thesis is to demonstrate a structured approach to strategic information systems (IS) planning. This thesis provides mid- and top-level managers at the Office of Naval Intelligence (ONI) with a guide for developing an information systems strategy and architecture that supports organizational goals outlined in the ONI Strategic Plan. By examining established information systems planning practices, architectural design methodologies, Department of Defense (DoD) guidelines, and published ONI organizational objectives, this thesis provides a guide through the decision-making process involved in strategic IS planning. This thesis presents a framework for developing a strategically aligned systems architecture that is specifically applicable to current systems development efforts at ONI.

At the enterprise level, the objective of this thesis is to link the strategic-planning vision and direction of ONI with a supporting information systems plan. Strategic IS planning practices provide the concepts and practical guidance for establishing the link between the fundamental business functions of an organization and its supporting information systems. Strategic IS planning must be an integral part of an organization's general planning process performed within a strategic framework. "Strategic advantages are gained when the organization is able to distinguish itself through lower costs, better products or services, or unique capabilities." [Ref. 1:p. 9] These advantages can be exploited by ONI or any organization that successfully maps its general strategic vision to a shared vision of the proper strategic use of information technology. "Few organizations can claim to have a widely shared vision of how they might best prosper in the Information Age." [Ref. 1:pp. 262-263]

At the work-group level, the objective of this thesis is to bridge the gap of individual understanding between those focused on the organizational mission and functional tasks (the users) with those charged with designing and providing supporting information resources. It attempts to provide the "big picture" to those who often feel the immediate impact of seemingly continual information systems modifications and technology advances.

> Many common shortcomings of information systems--such as technical elegance at the expense of relevance, hardware efficiency at the expense of flexibility . . . stem in part from the difficulties some technical managers have in seeing problems from the perspective of the user and the needs of the business. This can feed on itself, setting up a barrier to communications and cooperation between users and the technical staff. [Ref. 1:p. 14]

Hopefully, this thesis can serve as a vehicle for communication, coordination, and increased understanding among involved parties.

Though this thesis is written in response to research requirements that parallel systems development efforts at ONI, significant portions of this thesis are applicable to any large-scale organization, government or commercial, with a critical dependence on automated information systems. As with most strategic IS planning approaches, the purpose is to link business and information strategies to facilitate and enhance the most critical business functions. This research involved literature reviews and case studies associated with private business organizations. It examines several established strategic planning practices and demonstrates methodologies currently in practice within DoD. In the process, it presents a systematic method for resolving issues common to organizations with large information systems investments.

B. BACKGROUND

This thesis is being written for the Office of Naval Intelligence (ONI) located in Suitland, Maryland. ONI is responsible for the collection, production, and dissemination of maritime intelligence information in support of the Department of the Navy (DoN), joint and Naval operating forces and commands, the defense research and development (R&D) community, the Department of Defense (DoD), and the national command authorities and agencies. In support of its mission, ONI manages a large array of automated information systems that include both older technology mainframe computer systems as well as a more modern workstation environment. The computer systems support large databases and intelligence-specific applications supporting mission areas including scientific and technical intelligence and operational intelligence. An extensive communications architecture supports requirements to collect data, interface with other command and intelligence organizations and systems, and disseminate information to intelligence consumers.

Current DoD policy directs efforts for achieving compatibility and interoperability among Command, Control, Communications, Computers, and Intelligence (C4I) systems. Recent efforts focus on creation of joint intelligence and communications architectures across the Unified Commands, the individual Services, and DoD agencies. Further policy direction from the Director of Naval Intelligence (DNI) has consistently been in accordance with Department of Defense Intelligence Information System (DODIIS) and Common Operating Environment (COE) objectives. Additionally, the ONI Strategic Plan provides the vision and goals to ensure that Naval Maritime Intelligence resources are available to all users who need that information.

Given that the genesis of the new Global Command and Control System (GCCS) is the Joint Maritime Command Information System (JMCIS), the basis now exists to implement within ONI a truly interoperable, open systems, C4I architecture that will support national, theater, and tactical users. Therefore, as a matter of policy, all ONI systems development is being accomplished within the JMCIS architecture and its established systems development procedures. Over the last decade, ONI has sponsored several intelligence systems development efforts with the Naval Command, Control, & Ocean Surveillance Center (NCCOSC), Research, Development, Tests, & Evaluation Division (NRaD). Current efforts focus on design and implementation of a common architecture and structure that can accommodate unique ONI analytical requirements within the JMCIS framework. To ensure these unique requirements and organizational goals are carefully addressed, a structured strategic IS planning process is required. This thesis specifically addresses this requirement. [Ref. 2]

C. SCOPE AND METHODOLOGY

The main thrust of this thesis will be applying established principles of information systems planning to the architecture development effort at ONI. Specifically, the heart of the effort will include the development of a draft target architecture that will focus on mission critical systems at ONI, primarily those supporting intelligence production within the Intelligence Directorate (ONI-2). Additionally, it will present a framework for making critical migration path decisions that can be generically applied.

The methodology is structured on guidance provided by the DoD's Technical Architecture Framework for Information Management (TAFIM) Standards-Based Architecture (SBA) Planning methodology. This thesis is not intended to thoroughly address or demonstrate all aspects of the planning process described in the TAFIM. The SBA Planning process calls for a much more exhaustive approach to be conducted by an organizationally internal Architecture Working Group and Architecture Steering Committee with a trained facilitator. When conducted on an intensive basis with dedicated personnel and other required resources, the SBA planning process will typically require over one year to complete. That level of effort and coordination is clearly beyond the scope of this thesis. However, it is the intent of this thesis to demonstrate the validity of using the structured architectural approach presented by the TAFIM and other strategic IS planning concepts in concert with intelligence-specific IS planning guidance, provided through the DoD Intelligence Information System (DODIIS) program, to systematically address the issues, problems, and critical decisions faced by organizations attempting the strategic IS planning process.

In addition to an external literature review, thesis research included numerous personal interviews with mid- and top-level managers at ONI within both the Intelligence Directorate (ONI-2) and the Systems Directorate (ONI-7), as well as intelligence analysts (system users) within ONI-2. Two visits were made to ONI between December 1993 and June 1994. Additional interviews and coordination was performed with systems engineers at NRaD in San Diego during a February 1994 visit.

This research is intended, as much as possible, to present an *internal* focus with direct application to current systems development efforts at ONI. In a sense, this thesis is intended to be used as a companion guide in conjunction with research recently completed and presented to ONI in the thesis entitled "Downsizing Information Systems: Framing the Issues for The Office of Naval Intelligence (ONI)" by Lieutenant Peter M. Hutson in March 1994. His complementary research offers a more *external* perspective of relevant downsizing issues framed specifically for ONI. With an understanding of those issues as a backdrop, the internal planning methods then offered by this thesis provides decision-makers at ONI with a broad perspective of the strategic IS planning process.

D. OUTLINE OF CHAPTERS

1. Chapter II. Strategic Information Systems Planning

In this chapter, the concepts of strategic information systems (IS) planning are first presented in the broader context of strategic business planning. Specifically, the analytical techniques of Critical Success Factors and Pressure Point Analysis are reviewed. These common concepts are narrowed to the IS field with an explanation of the architectural approach to strategic IS planning. Continuing toward a more structured approach, the specific methodologies offered by DoD's Technical Architecture Framework for Information Management (TAFIM) and DoD's Intelligence Information System (DODIIS) guidelines are examined. This chapter prepares the reader with a broad understanding of strategic IS planning and a specific understanding of the methodologies that structure the development of ONI's systems architecture.

2. Chapter III. Initiation and Architecture Framework

In this chapter, the structured methodology offered by the architectural approach to strategic IS planning is initiated. The chapter presents the issues that initiate the planning process within an architecture framework. ONI's strategic planning documents and mission statements are examined. Strategic IS initiatives that directly impact ONI systems development are also reviewed. Central to this chapter is the development of initial IT Principles for ONI that will guide the systems development and architectural planning efforts. Finally, key issues that will impact the overall architecture process are presented to set the stage for further phases in the planning and development process.

3. Chapter IV. Baseline Characterization

This chapter presents a high-level baseline characterization of the IS environment currently supporting the critical mission / business functions at ONI. The baseline environment is presented from four separate views: work organization view, information view, application view, and technology view. Applications, systems, and databases that directly support ONI intelligence analysts are presented.

4. Chapter V. The Target Architecture

This chapter presents a draft target architecture to guide systems development and evolution at ONI. This chapter specifically addresses the Joint Maritime Command Information System (JMCIS) architecture. A thorough understanding of the JMCIS architecture is essential to guide the architecture development efforts at ONI. Application of the JMCIS architecture concepts to ONI system requirements are first presented in the chapter.

5. Chapter VI. Opportunity Identification

This chapter builds on the basic understanding of the target architecture by identifying the opportunities presented by JMCIS. The opportunities are presented with regard to the strategic goals and IT principles of ONI. Opportunities are identified which, once implemented, can demonstrate the value of the architecture and provide immediate benefits to the organization.

6. Chapter VII. Migration Analysis

This chapter presents a framework to assist decision-makers in the process of analyzing a migration path toward the target architecture environment. The chapter first defines many of the terms required to properly discuss and further analyze a migration plan. With the terminology as a back drop, this chapter then specifically addresses some concerns regarding the migration plan for ONI systems. Finally, this chapter offers a suggested framework to properly evaluate and select a migration plan. A generic decision framework is presented that is a functionally-oriented, capability-based approach. It is intended to be a useful, step-by-step method that produces valuable information about the migration path selected. The framework is presented to offer decision makers a structured approach to evaluating migrations options.

II. STRATEGIC INFORMATION SYSTEMS (IS) PLANNING

A. STRATEGIC PLANNING AND ANALYSIS FOR IS

1. Definition

Strategic planning is defined in the literature in many ways. It takes on a variety of meanings depending on the context or business environment in which it is used. In the commercial sector, one might define strategic planning as "planning in response to corporate business initiative." [Ref. 3:p. 2] Military planners define strategic planning as the large-scale, long-range utilization and deployment of the nation's forces to ensure national security objectives. In the broadest sense, however, planning is simply "deciding in advance what is to be done." And *strategic* planning is making those advance decisions with concern for the fundamental purpose and direction of the entire organization. [Ref. 4:p. 108]

Strategic *information systems* (IS) planning is a form of strategic planning intended to align an organization's information systems with it's critical strategic goals and supporting mission specific functions. "The objective of strategic information systems planning is to define the explicit connection between an organization's business plan and its systems plan to provide better support of the organization's goals and objectives and closer management control of critical information systems." [Ref. 3:p. 2] The basic purpose is to link the business and information strategies. Establishing a link between fundamental business needs and the supporting information systems requires an explicit understanding of those needs. The consensus of many companies having strategic IS planning activities is that planning, set in a strategic framework, will allow decisions to be made today which will better prepare them for the future. Strategic IS planning must therefore be an integral part of an organization's general planning process and be performed within this strategic framework. [Ref. 3:p. 9]

2. Elements of Strategic IS Planning

The concept of strategic IS planning is demonstrated in the process of systematically thinking through a business situation, considering both internal and external forces that may impact the business, anticipating the changes that information technology will effect on the business, and developing a series of options, or alternative *objectives*, from which management can select a course of action. Business situations are described in terms of *issues*, which are unresolved management concerns. The process of thinking through these issues is called *analysis*. A course of action may then be chosen from the alternative objectives resulting in an *implementation* or *action plans*. [Ref. 3:p. 2]

Issues and *objectives* are the key elements of strategic IS planning. The purpose of strategic IS planning is to help resolve the organization's business *issues* and attain the desired *objectives* by setting IS objectives and accomplishing them. It helps to resolve the *issues* by the selection of certain options from among various possibilities that have been analyzed while considering the business factors involved. Strategic IS planning involves a disciplined thinking process resulting in a structured communication of ideas. Through strategic IS planning, strategic business issues are translated into specific IS *action plans*. [Ref. 3:pp. 4-11]

3. The Strategic IS Planning Process

The process of strategic IS planning is procedurally described throughout literature. Wading through all the advice on strategic planning for IS can be difficult. There are many differing opinions and resultant frameworks to choose from. However, they all similarly argue that an organization's primary concern should be to integrate the strategic IS planning process with the general strategic planning process. This section presents a high-level view of the strategic IS planning process that is common to most frameworks.

The first step common to most strategic IS planning processes is a thorough analysis and understanding of the organization's general strategic goals as laid out in a strategic plan. IS objectives are set only *after* strategic analyses are conducted. The IS planning process starts with *business objectives* and not IS objectives. The "strategy" referred to should always be the strategy of the organization for which the information resources support, not the strategy of the information services group itself. This initial step typically includes a review of the organization's business plans in order to clarify corporate objectives and identify critical mission / business functions. Strategic IS planning must begin with the development of a framework of business issues and objectives to properly align the IS activities with the business activities. From this framework, essential information needs can be established and future requirements identified. [Ref. 3:p. 29]

Also among the first steps common to IS planning is an internal analysis to evaluate how information resources are currently supporting the critical business functions of the organization. Characterizing the information systems and technologies currently installed provides a basis on which to begin the IS planning process. This step also serves to identify weaknesses in the current systems architecture that need to be closely examined from a strategic perspective during the IS planning process.

The next step in strategic IS planning is born out of the first two. With an understanding of the critical business functions and a characterization of the currently available information resources, the next step in the planning process should develop and describe a goal or target IS environment that will support the strategic information requirements of the organization. A strategically designed IS infrastructure is developed through a shared vision among both technical and operational personnel of how information technology can support the user.

> Lack of a shared vision inhibits the strategic use of information technology. The technology has the potential to bring about profound changes, but success will be elusive without some common understanding of what the organization wants to achieve and how [information systems] can contribute. [Ref. 1:pp. 262-263]

With an understanding of the current state of IS within the organization and a vision of where the organization wants to go, identification of available opportunities that allow attainment of the target IS environment is required. Various IS opportunities that fulfill the requirements of the target environment are recognized as potential alternatives during this step in the planning process. This step involves the generation of feasible alternative courses of action with an analysis to determine what impact the alternatives may produce. Determining the most strategically beneficial option is the goal of this phase in the planning process.

Opportunity identification and selection is generally followed in the strategic IS planning process by a plan to implement the selected alternative. This step typically involves a planned transition phase in which the current IS environment is "migrated" toward the target environment using the selected opportunity. This final phase is often referred to as operational IS planning where strategies to handle specific IS projects and activities are devised and included in the operational planning cycle. Strategic IS planning is in direct response to corporate business initiatives. It is usually concerned with specific IS projects in support of specific business plans of high priority. In this manner, strategic business issues are translated into specific IS action plans through the strategic IS planning process. [Ref. 3:p. 6]

The process of strategic IS planning is described in many different ways with the basic steps arranged in various orders. The process is inherently flexible and changeable because, by its nature, strategic planning is concerned with special situations that have differing time demands and a wide range of management interest and urgency. While the overall process must be flexible enough to accommodate new technologies, each part in the process is itself well structured. It is the structured approach of each step in the process that ensures the critical alignment between the strategic business plan and the specific IS action plans. [Ref. 3:pp. 12-26]

4. Strategic IS Analysis

Strategic planning often requires diverse planning techniques and data analysis methods at different phases of the planning process. Analytical methods are required to resolve complex issues into settled, or final, objectives. In general, strategic planning is the method for settling issues, resolving unanswered questions, and refining the results of strategic analysis into a statement of objectives. Several methods may be required to perform this analysis, including business plans analysis, environmental analysis, forecasting, trend analysis, internal analysis, risk analysis, contingency analysis, and economic analysis. At the end of a successful strategic analysis, objectives are set and a strategic plan is prepared. Decision-oriented planning is facilitated through the use of detailed analysis in the strategic planning process. [Ref. 3:pp. 19-20]

Several analysis techniques have been introduced for use in strategic IS planning. For example, the use of Critical Success Factors (CSF) in planning was first proposed by Dr. John Rockhart of the Center for Information Systems Research at MIT. There have since been numerous articles published on the subject and many successful uses of the approach. The methodology requires management to define the organization's Critical Success Factors, limiting the number of factors to "the relatively few things that an organization judges that it must do well to thrive." [Ref. 1:p. 290] Developing a set of Critical Success Factors has become a popular way of extracting top management's key concerns, giving uniform direction to the planning process, and stating general goals while the outcome is still technically ill-defined. The high-level approach of this technique is appropriate for strategic-level IS planning.

Another high-level analytical technique is called Strategic Pressure Point Analysis (PPA). This technique also provides a way of gathering and presenting information that focuses on issues of particular interest to management, rather than on the specific technical problems. The "pressure points" are considered those key external factors producing the most pressures on the current status of the IS infrastructure. One apparent strength of PPA can been seen in the model provided for organizing and clearly presenting the information to help decision makers view the various pressures influencing the decision process. Figure 1 is an example of a business-oriented PPA model depicting the various pressure points considered.

Pressure Point Analysis provides a simplistically clear analytical approach to planning embodied in four fundamental questions concerning the role of IS in an organization:

- Where are we?
- Why should we change?
- What could we do?
- What should we do?

The search for and display of answers to these questions comprises the sum and substance of Strategic Pressure Point Analysis. Answering these fundamental questions incorporates the basic steps common to all strategic IS planning processes. The steps can be summarized as producing a profile of existing IS functions (Where are we?); identifying the issues demanding a solution (Why should we change?); listing strategic alternatives (What could we do?); and recommending a course of action (What should we do?). [Ref. 3:p. 69]

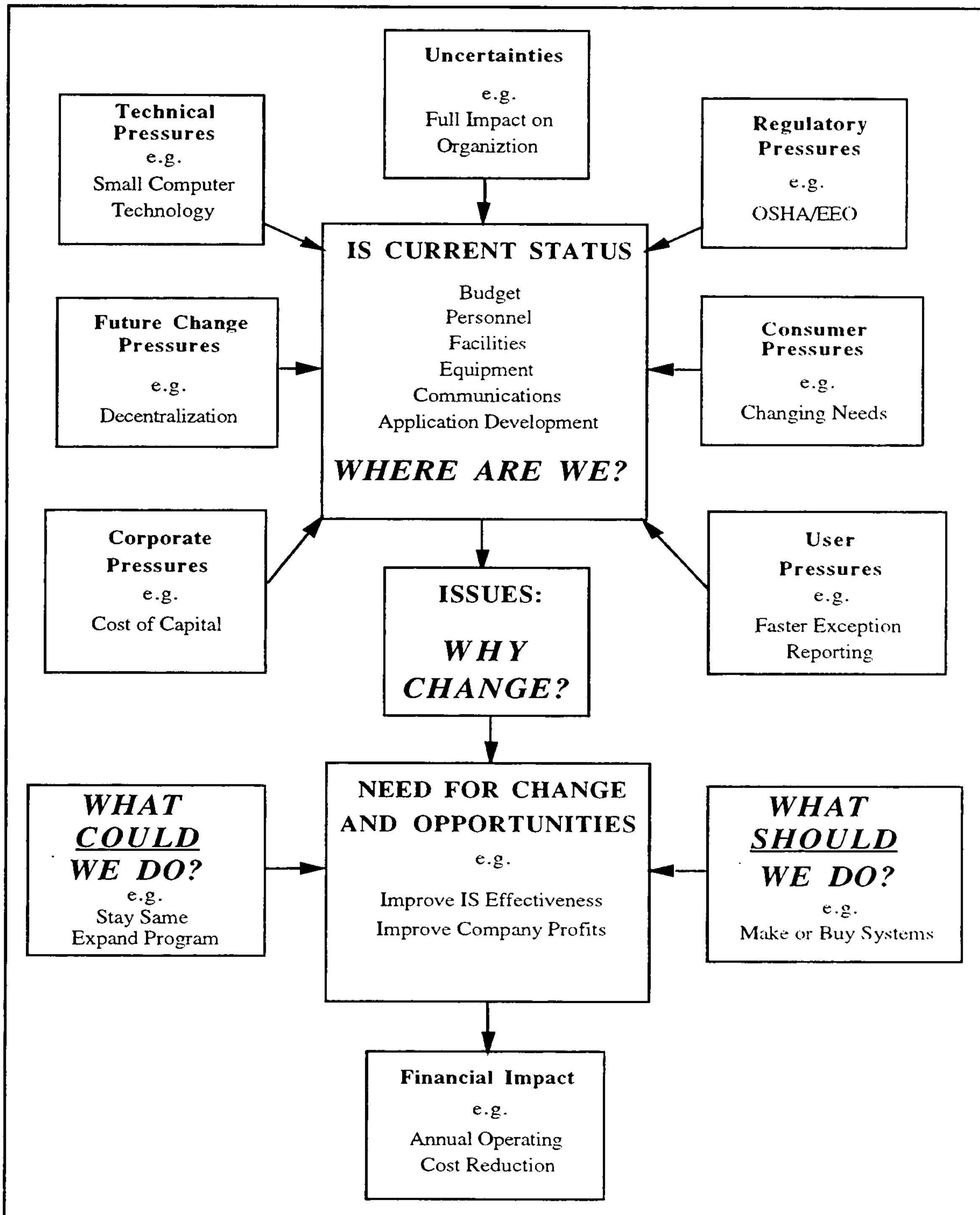

Figure 1: Strategic Pressure Point Analysis Chart [Ref. 3:p. 68]

5. Outcome of Strategic IS Planning

The strategic IS planning process provides an opportunity for an organization to consider explicitly how it should exploit the capabilities of information technology. If done successfully, this process should produce a plan that provides the following:

- A description of a desired future IS capability required to support the strategic needs of the organization;
- Guidance for current actions aimed at achieving the plan;
- A framework and focus for organized problem solving;
- A means for communication and coordination among involved parties.

[Ref. 1:pp. 259-260]

Typically, various documents are produced during the planning process. The documents that come from all types of planning are created to define objectives, analyze alternatives, and describe the directions which should be taken. The documents specifically serve to communicate the strategic IS plan. Documents describe the systems architecture, the strategic alternatives, the options considered, and the equipment and software strategies. Together they form the strategic IS plan.

A useful strategic IS plan must provide guidance for making relatively short-term decisions on such matters as the allocation of resources and the selection among technical alternatives. A plan that has no bearing on these decisions is too future-oriented or too irrelevant to contribute much. The strategic IS plan must also take a longer-term view, because it takes a series of purposeful actions to put into place the kind of IS infrastructure that can support the organization's strategic objectives. Stated differently, the objective of strategic IS planning is to arrive at near-term decisions that coincide with the long-term direction of the organization. [Ref. 1:p. 260]

B. ARCHITECTURAL INFORMATION SYSTEMS (IS) PLANNING

Recent IS planning strategies focus on structured methods to guide the planning and analysis process. While previous strategic IS planning practices were derived from generally accepted business planning techniques, strategic IS planning has required a more structured approach to ensure a successful alignment of the business and IS plans. Today's IS planning techniques have an apparent systems engineering influence. Systems analysis techniques have blended with more traditional organizational analysis to constitute the modern strategic IS planning process. These techniques include information modeling, business process re-engineering, and systems architecture. The merger of the behavioral science approach to organizational planning with the systems engineering approach to systems design has resulted in the architectural approach to strategic IS planning. "For the 1990s through the 2000s, information systems architecture and the architectural approach as the main methodology for strategic systems planning are recognized as the key issues for IS." [Ref. 5:p. 102]

1. Definition

The term *architecture*, long used to describe aspects of building design, has been applied to technical systems for about a generation. A technical systems architecture defines components, interfaces, services, and the framework in which they are incorporated. An IS architecture is a set of components and a specification of how these components are connected to meet the overall requirements of an information system. Components provide either information processing or communications services. Architecture is not necessarily a diagram of the components or a set of diagrams. "Rather, it is a set of company policies and rules, that when followed, are expected to lead to the information systems environment that is desired." [Ref. 6:p. 182]

An analogy can be useful in understanding what an architecture is and why it is important. An architecture typically allows designers (architects) to lay out the plans for a project in terms that builders or developers can understand and use them to guide the construction process. Like the building architecture, the plans include provisions for the various services to be offered in the building, such as electrical power, plumbing, communications wiring, stairwells, elevators, etc. They must also provide the overall design of the building. An architectural plan must also consider zoning laws, regulations and standards for building usage. It must also consider the entrances and exits, layout of the equipment which may be housed in the building, and the type of construction material needed to meet the planned usage requirements of each area of the building. The architecture must ensure that components of the building fit together to meet the needs of the prospective tenants and the surrounding environment. It must also have the ability to evolve with the changes over time such as the need for expansion or for alternative uses. [Ref. 7:Vol. 4,pp. 1-2 to 1-3]

The architecture does not, however, concern itself with details such as the specific color of carpet a given tenant may want, or exactly how each person's desk will be oriented. Rather, the architecture concerns itself with providing a flexible, adaptable infrastructure to meet these varying needs without tearing down the building and starting over. This is accomplished by adhering to solid principles of architecture design, by developing a set of blueprints (or frameworks) for the building's appearance and layout, and by setting some basic standards for the construction teams to follow as they implement the plans. The framework serve as a starting point to begin construction. [Ref. 7:Vol. 3,p. 5]

Similar to the building architecture, an IS architecture serves as the underlying framework that defines and describes the IS requirements of an organization and its primary functions. Meeting these requirements will allow the organization to attain its business objectives. The IS architecture provides the structure for information, applications, and the technological means. It describes the groupings of components, their interrelationships, the principles and guidelines governing their design, and their evolution over time.

> The bottom line on architectures, for buildings and for [IS], is providing a minimum, but rigorous, set of guidelines and standards which will allow the building (or information systems) to be developed in a way which will allow the most flexibility for the tenants (or system users) while constraining the detailed designs enough to ensure that the desired style and characteristics of the building (or the computing environment) are maintained over time. [Ref. 7:Vol. 4, p. 1-5]

2. Principles of Systems Architecture

There is a direct analogy in the principles of IS architecture for each of the more general architecture points discussed above. The architectural principles for a building define the overall style of the building and its general characteristics. With these architectural principles, one gets a fairly good idea of the kind of building and some of the constraints which will be placed on the construction. In IS architecture, the principles provide a similar mechanism for defining the kind of information systems that will result. The IT architectural principles are the foundation for decision making about the general style of computing and technology usage for the organization.

An example IT principle might be:

> To the extent possible, similar business functions will be supported by common systems which will support all physical locations. These systems will be run locally, within each plant location, but will be maintained and updated from a central location. The systems will be developed within an industry standard environment and will be interconnected for data sharing via a series of interconnected telecommunications networks, which will communicate using industry standard protocols. Access to all systems will be via intelligent workstations connected to the network and using a set of common user interface standards. [Ref. 7:Vol. 4, p. 1-4]

This principle would then be used to guide the development of models and associated specifications for the way the organization will use IS. With this principle, the style of computing and communications is defined with enough depth to allow appropriate detailed design work to begin and developers selected.

As the construction begins, some specific decisions will have to be made about vendors as well as the details of construction for specific user needs. In the construction planning phase, the architecture still forms the framework for decision making, but more detailed plans will have to be developed for each user's specific requirements. Here, the cost of materials, durability requirements, specific equipment locations, and office layout must be considered. A detailed design must be developed with specific cost estimates, time to complete, vendors to be used, etc. This goes beyond architectural planning but must remain consistent with the architectural principles and blueprints for the overall building.

3. Elements of Architectural IS Planning

With the building architecture analogy as a backdrop, architectural IS planning can be defined "as the art and science of transforming a functional need for computer-based systems into a planned and organized framework which supports integration and enables systems design and delivery." [Ref. 7:Vol. 4,p. 1-5] The architectural IS planning process requires the definition of components or "building blocks" and ways to describe the relationship among components. The architecture provides the link between identifying a strategic opportunity to apply computer solutions and choosing the best available solution.

In order to link the strategic functional requirements of an organization to the supporting IS infrastructure, the IS architecture must reflect four different views of the organization. These four views are:

- <u>Work organization view</u>. The work organization view describes the major operations that are performed by work groups in support of mission / business functions. This view should address how the planned system will impact work activities, change skill requirements, affect functional operating locations, and eliminate or reduce manual support.

- <u>Information view</u>. The information view describes the critical information used by the organization and the relationships among collections of information (databases). This view should address the information / databases that are required to operate the function, and the format and volume of information involved.

- <u>Application function view</u>. The application view shows which functions of the organization can be supported by IS applications. It provides a high-level description of these applications and describes logical dependencies and relationships among application areas. This view should describe what types of application functions are required to support the organization and associated users, how functions will be grouped and interfaced, and what usage levels are anticipated. This view defines the scope and interfaces of applications and provides the basis for detailed design.

• Technology view. The technology view is used to describe the enabling infrastructure. To provide the necessary linkage to the work organization, information, and applications architecture views, the technology view can further be described in terms of generic "building blocks". This view should describe what types of technology services are required and how should they be distributed to various types of technology platforms, how these services and platforms will be networked, and what standards and guidelines are required to support integration. [Ref. 7:Vol. 4]

The work organization view forms the critical foundation on which the strategic IS planning process can begin. The application and information views are used in tandem to define the targeted applications and information that will support the organization. Together they drive the requirements for technology. It is important that standards-based architectures reflect a balance of these four views of their relationship.

4. Goals of an IS Architecture

Given an understanding of the purpose and elements of architectural IS planning, an IS architecture must address three goals:

• Provide a means of cost effectively organizing information and its technologies to support the organization's objectives;

• Improve the effectiveness of IS in delivering new capabilities to the organization;

• Facilitate continual evolution of the IS infrastructure and solutions over time. [Ref. 7:Vol. 4,p. 1-10]

Similar to other strategic IS planning techniques, the common questions addressed by the architectural IS planning process are:

• How can we define an IS architecture which meets the functional vision of the organization?

• How do we get there from here?

C. DOD's TECHNICAL ARCHITECTURE FRAMEWORK FOR INFORMATION MANAGEMENT (TAFIM)

1. Overview

The Defense Information Systems Agency (DISA) Center for Architecture began publishing a multiple volume of systems architecture development guidelines in November 1993. These documents comprise the DoD Technical Architecture Framework for Information Management (TAFIM) series. The purpose of TAFIM is to provide "an enterprise-level guide for developing technical architectures that satisfy specific functional requirements." [Ref. 7:Vol. 1,p. 3] The TAFIM is not intended to provide a specific systems architecture. Rather, it provides standards and design concepts that can be used to guide the development of technical architectures that meet specific mission requirements. The TAFIM provides system architects and designers with "a basis for developing a common target architecture to which systems can migrate, evolve, and interoperate." [Ref. 7:Vol. 1,p. 3]

Like other strategic level planning methodologies, TAFIM is independent of the technical details regarding mission-specific applications and their associated data. The specific architectures for specific missions and functions will be developed using the standard architecture guidance and development methodologies provided by the TAFIM. Although high-level in nature, the TAFIM approach assumes that all information systems must interoperate at some time. It is intended that through the widespread use of a standard methodology such as the TAFIM provides, interoperability among the various systems will increase, providing users with improved services needed to achieve common functional objectives. Proper application of the TAFIM is intended to:

• Promote integration, interoperability, modularity, and flexibility;

• Guide acquisition and reuse; and

• Speed delivery of information technology and lower its costs.

[Ref. 7:Vol. 1,pp. 3-4]

The TAFIM defines an information system to include support and mission-oriented applications, computing platforms, and communications networks. The current DoD IS infrastructure consists largely of stovepipe, single-purpose systems that are costly to maintain. These systems reflect many varied approaches to migrate toward open systems with each one progressing on its own path with limited attention to interoperability. In the absence of DoD-wide systems architecture guidance, various DoD organizations and agencies have developed a wide range of architectures to manage and control their IS infrastructures. Reference models, information architectures, communications architectures, mission architectures, and various other architectures are now used to manage the design and development of information systems within DoD. The TAFIM was developed to provide a single IS architecture framework to integrate these various efforts and promote common systems design, acquisition, and reuse principles throughout DoD. The TAFIM provides a DoD-wide framework to manage multiple IS architecture initiatives. [Ref. 7:Vol. 1,pp. 1-3]

The TAFIM provides a set of volumes to guide the evolution of the DoD's IS architecture. Version 2.0 of the TAFIM Volumes are listed below:

• Volume 1: Overview.

• Volume 2: Technical Reference Model - provides the conceptual model for information system services and their interfaces.

- Volume 3: Architecture Concepts and Design Guidance - provides concepts and guidance needed to support the development of technical architectures in the DoD.

- Volume 4: Implementation Manual - provides a standards-based architecture planning methodology to help architects, technical integrators, and developers plan and build information systems that meet mission, functional, and application area requirements. The methodology provides a translation of functional requirements to the selection of services, standards, components, configurations, their phasing, and the acquisition of products that implement them.[Ref. 7:Vol.1,p. 9]

- Volume 5: Support Plan - provides guidance on how to use the TAFIM in the acquisition of IT and IM products.

- Volume 6: DoD Goal Security Architecture - provides security requirements commonly found in DoD organizations with regard to missions and mission threats. (Unpublished)

- Volume 7: Standards Profile and Implementation Guidance - provides DoD profile of standards. (Unpublished)

- Volume 8: DoD HCI Style Guide. (Unpublished)

[Ref. 7:Vol. 1,pp. 9-10]

2. Architectural Guidance

The TAFIM Volume 4 provides a Standards-Based Architecture (SBA) Planning Guide which defines a common framework for strategic and architectural IS planning among all levels of DoD. The TAFIM Volume 4 is intended to serve as a key element of the DoD's Corporate Information Management (CIM) initiatives (to be further discussed in Chapter III). It serves as the DoD-wide strategic IS planning guidance for the implementation of a computing and communications architecture that will support portability, scalability, and interoperability of applications. The CIM initiatives are reaffirmed by Deputy Secretary of Defense William J. Perry's policy memorandum of 13 October 1993 entitled "Accelerated Implementation of Migration Systems, Data Standards, and Process Improvement." It calls for all DoD components to begin migration from legacy to target systems in such a way "that migrate the system toward an open system environment and a standards-based architecture defined by the DoD Technical Architecture Framework for Information Management (TAFIM)." [Ref. 7:Vol. 4,p. 1]

3. TAFIM Methodology

The TAFIM SBA Planning methodology was developed to assist in planning IS architectures within a functional unit or department within the DoD. The approach is also intended to be useful when applied at a lower or sub-department level providing a more detailed view of the architecture. The SBA planning process, like other strategic IS planning methodologies presented, provides a mechanism for translating the mission critical business functions of an organization into specific IS actions which are derived through the use and implementation of the entire TAFIM SBA planning process. Figure 2 represents the standards-based architecture planning and implementation cycle outlined in the TAFIM Volume 4. Similar to other strategic IS planning processes, the SBA planning process consists of seven distinct, but interdependent, phases. Each phase produces specific documents as deliverables which then guide the subsequent phase(s). The phases are briefly described below:

a. Phase One: Initiation and Architecture Framework

This phase in the architectural planning process is direction-setting in nature. The methodology begins by initiating the process within the host organization. This orientation phase involves reviewing (or in some cases developing) a set of strategic objectives for the organization. The strategic business plan is reviewed (or built) during this phase to establish a understanding of the organization's strategic vision. A set of IS architecture principles is developed to establish what are believed to be good architecture practices for the organization. [Ref. 7:Vol.4,p. 5]

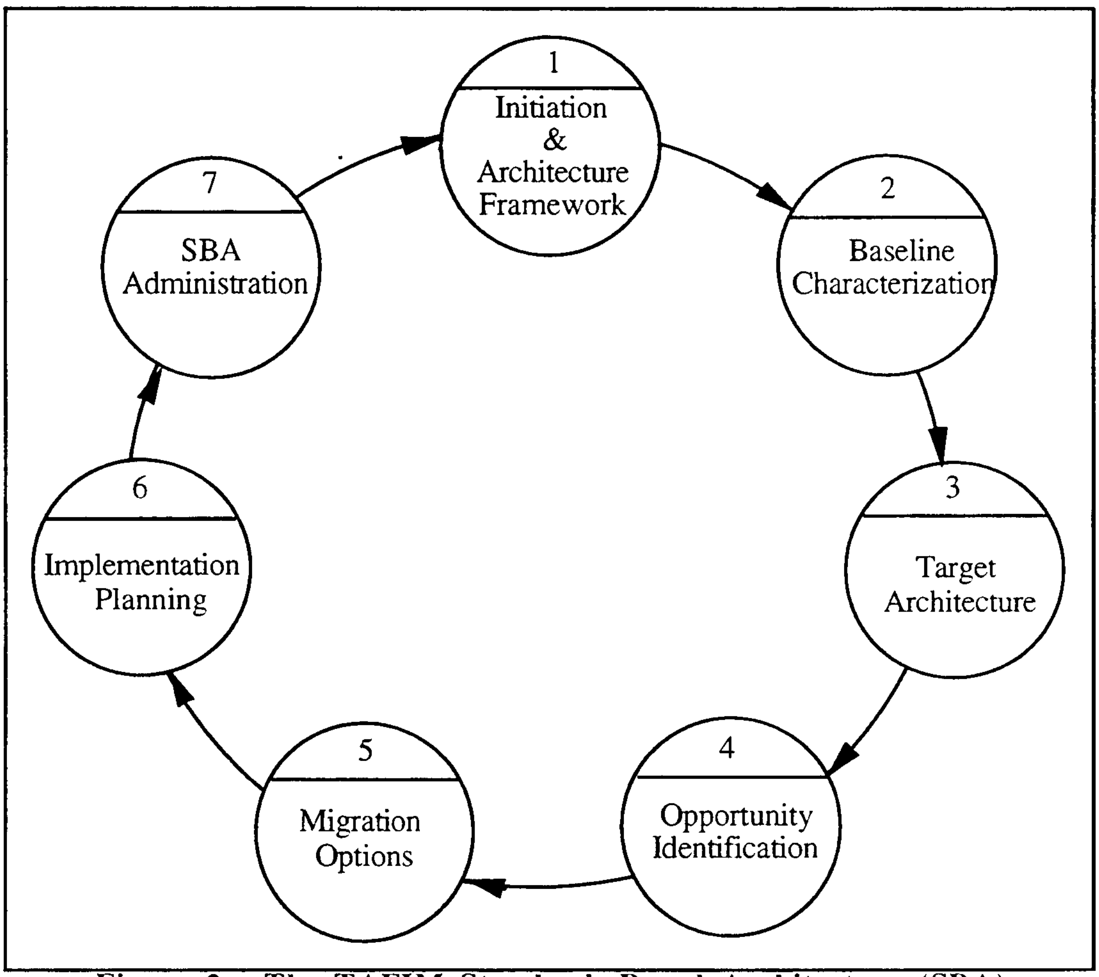

Figure 2: The TAFIM Standards-Based Architecture (SBA) Planning Process [Ref. 7:Vol. 4,p. 4]

b. Phase Two: Baseline Characterization

The purpose of this phase to determine the organization's current IS environment. It is used to establish a baseline, or starting point, for architecture development. The baseline characterization provides a useful means for organizing and presenting the current IS status. It results in a "picture" of the existing architecture along four key dimensions, or views: work, information, applications, and technology. The term "characterization" is used because the data gathering and analysis are not exhaustive. It is not necessary, nor is it desirable, to expend the time and effort to document every detail of the current architecture. Only enough detail is gathered to allow informed decisions to be made with regard to the desired target architecture. [Ref. 7:Vol. 4,p. 5]

c. Phase Three: Target Architecture

Target architecture development is the heart of the SBA planning process. The target architecture specifies the new IS environment and highlights the key opportunities for improvement over the baseline. The goal of this phase is to define a target architecture that can be used to support and thus achieve the strategic vision of the organization. The architecture that is actually implemented will likely be a blend of the baseline and the target with architectural principles as the foundation.

d. Phase Four: Opportunity Identification

This phase moves the architecture out of the conceptual world into one where the practical realities govern implementation. In this step, short-term opportunities are identified which, once implemented, can demonstrate the value of the target architecture and provide some immediate benefits to the organization. In addition, IS projects that are necessary to achieve the target architecture are identified and described in some detail.

e. Phase Five: Migration Options

This phase links the reality of the present IS environment with the desirability of the target architecture by establishing steps that represent practical migration stages. IS projects recognized in the previous step as opportunities are analyzed with best alternatives identified. The objective of this phase is to develop a prioritized set of project initiatives which, when completed, will move the organization from the current state to the target architecture. [Ref. 7:Vol. 4,p. 6]

f. Phase Six: Implementation Planning

This phase results in a detailed implementation plan for the first steps of the migration effort. The plan describes the first actionable projects that establish the basis for each successive phase of the target architecture implementation. Milestones are established and resource requirements defined. [Ref. 7:Vol. 4,p. 7]

g. Phase Seven: SBA Administration

This phase is intended to keep the architecture current and meaningful by continuously improving it. It reflects the need to modify architecture decisions in response to unforeseen changes in business directions or advances in technology, making adjustments as required. This phase is an ongoing process intended to measure and monitor project problems and architecture compliance. [Ref. 7:Vol. 4,p. 7]

4. Resource Requirements and Critical Success Factors

The SBA planning process presented by the TAFIM offers an architectural approach to strategic IS planning. It has many similarities to strategic IS planning techniques previously discussed. The TAFIM guidelines provide suggestions for individual organizations to tailor the SBA Planning requirements to best fit local resourcing, size, and timing constraints.

Critical to the success of this planning process is the adoption of a resourcing strategy supported at the highest levels of the organization. The SBA Planning process requires an Architecture Working Group (AWG) to be formed. This core team should consist of four to six mid-level managers and IT personnel from the functional areas. This team will develop the overall project plan and facilitate the SBA process. Key players must be involved. Additionally, the process requires formation of an Architecture Steering Committee (ASC). This group should also consist of a mix of IT and functional area experts that can provide expertise and guidance to the project.

TABLE 1: SBA PLANNING PROCESS CRITICAL SUCCESS FACTORS

SUCCESS FACTOR	*DESCRIPTION*
Business driven	Use the architecture process to reinforce key operational and business drivers.
Participative process	Involve teams of architects, planners, and managers directly in the creation of deliverables to establish corporate "buy-in."
Fast paced	Set schedules such that deliverables arrive within weeks, not months. Show early results.
Presumptive resolution	Do not get bogged down if facts or information are not available. Be presumptive, make the best guess, and document assumptions.
Architecture, not design	Avoid too much detail. Focus on architecture decisions and save some creative work for the designers to follow.
Minimum set	Do not set out to establish standards for everything in sight. Focus on those where key infrastructure is involved.
Key deliverables	It is more important to produce results which everyone can abide by than to follow specific processes or methods. Use the framework but be creative and experimental with methods using standard DoD tools and techniques.
Open, non-secretive	Do not hide the team away and stamp everything "confidential!" Invite participation and circulate drafts for review and discussion.
Ongoing process, not event	This is not intended to produce a shelf document. Create ongoing processes for updating and reviewing are critical.

[Ref. 7:Vol. 4,p. 8]

The SBA planning process is organized around the seven phases described. Ideally, when conducted on an intensive basis, these phases will require approximately one year to complete. The internal organization of the AWG and ASC, coupled with the time requirements, obviously calls for a strong commitment and support at the executive level of the organization. Additionally, the process calls for a trained group facilitator. Group facilitation skills, interview skills, general functional area knowledge, IT knowledge, and project management skills should all be considered required staffing skills for the AWG and ASC. As an final overview of the TAFIM methodology, Table 1 presents a list of the associated critical success factors for the seven phases of the SBA Planning process.

D. DOD INTELLIGENCE INFORMATION SYSTEM (DODIIS)

1. Overview

The Department of Defense (DoD) Intelligence Information System (DODIIS) is a national program comprising "the aggregate of personnel, procedures, equipment, computer programs, and supporting communications of the Department of Defense which support the timely and comprehensive preparation and presentation of intelligence . . . to military commanders and national-level decision makers." [Ref. 8] The DODIIS program is intended to facilitate the flow of information between members of the defense intelligence community by providing analyst access to and maintenance of databases and services for file transfers, information dissemination, and analyst-to-analyst exchanges (E-Mail). [Ref. 9:p. 1-1]

DODIIS has generally been understood to encompass those automated information systems (AIS) and associated resources funded all, or in part, by the General Defense Intelligence Program (GDIP). DODIIS has evolved from a series of individual systems development efforts into an increasingly interdependent set of subsystems which interact to provide integrated data handling support for the entire defense intelligence community. Additionally, the DODIIS program's management structure ensures that information systems developed and acquired for the defense intelligence community conform with current systems development principles and comply with specific guidance provided by the Congress and DoD in general. The DODIIS program has thus evolved into a comprehensive management plan providing strategic IS architectural guidance that is specifically tailored for defense intelligence organizations while complementing and complying with the general DoD IS planning guidance.

2. DODIIS Program Guidance

The DODIIS program was established in 1977 by the Joint Chiefs of Staff under Defense Intelligence Agency (DIA) management in support of the GDIP. Since initiation of Corporate Information Management (CIM) within DoD in 1990, top-level oversight of the DODIIS program, systems, and resources has been the responsibility of the Assistant Secretary of Defense for Command, Control, Communication and Intelligence (ASD/C3I). Other national agencies exercise influence over how DIA manages and implements the DODIIS program. DISA implements ASD/C3I policy with respect to information technology standards, data administration, and central acquisition standards for information technology requiring DIA compliance. DISA also manages the operation of the entire DoD information systems infrastructure, including the existing Defense Data Network (DDN) and its Special Compartmented Information (SCI) portion known as the Defense Secure Network 3 (DSNET3). Other agencies have controlling roles related to the intelligence systems and programs they manage, as in the case of the Central Intelligence Agency (CIA) and the National Security Agency (NSA). [Ref. 9:p. 1-2]

DIA is primarily responsible for planning, programming, and implementing DODIIS within the GDIP resource process. This responsibility is directed by the DODIIS Management Board (DMB) which is chartered by the Director of DIA and the Service

Intelligence Chiefs. The DMB is responsible for developing the management process for the DODIIS program. The DMB provides documented guidance to organizations seeking to develop information systems and components that support the requirements of the defense intelligence community. This management structure is intended to implement the strategic IS planning for the DODIIS program. The structure has been developed to enable the defense intelligence community to plan, design, develop, implement, and manage AIS components of the DODIIS program. [Ref. 9:p. 2-1]

3. Architectural Methodology

While the DODIIS program ensures compliance with emerging DoD-wide technical standards and implementing policy such as that provided by the TAFIM, the methodology for developing and migrating to an IS architecture specifically for an intelligence organization requires an additional review of the DODIIS guidance. In particular, the DODIIS Site Transition Methodology (DSTM) outlines a process for planning and managing a site's transition to an architecturally consistent DoD-wide guidance. A brief overview of this methodology is provided.

Like a common site implementation methodology, the DSTM is a standard planning approach for the acquisition and evolution of an IS architecture. The methodology begins with development of an objective site architecture, documentation of the current baseline, and development year-by-year plan for transition from the baseline to the objective. Figure 3 provides an overview of the transition methodology. This process follows similar procedures offered by other planning methodologies with the order varying slightly. It begins with development of an objective site architecture, or target architecture.

The process then calls for the current site architecture or baseline to be documented using the same format as the objective site architecture. Systems currently on site will evolve towards the objective architecture. Documentation guidance is provided by the DSTM. [Ref. 10:p. 3-1]

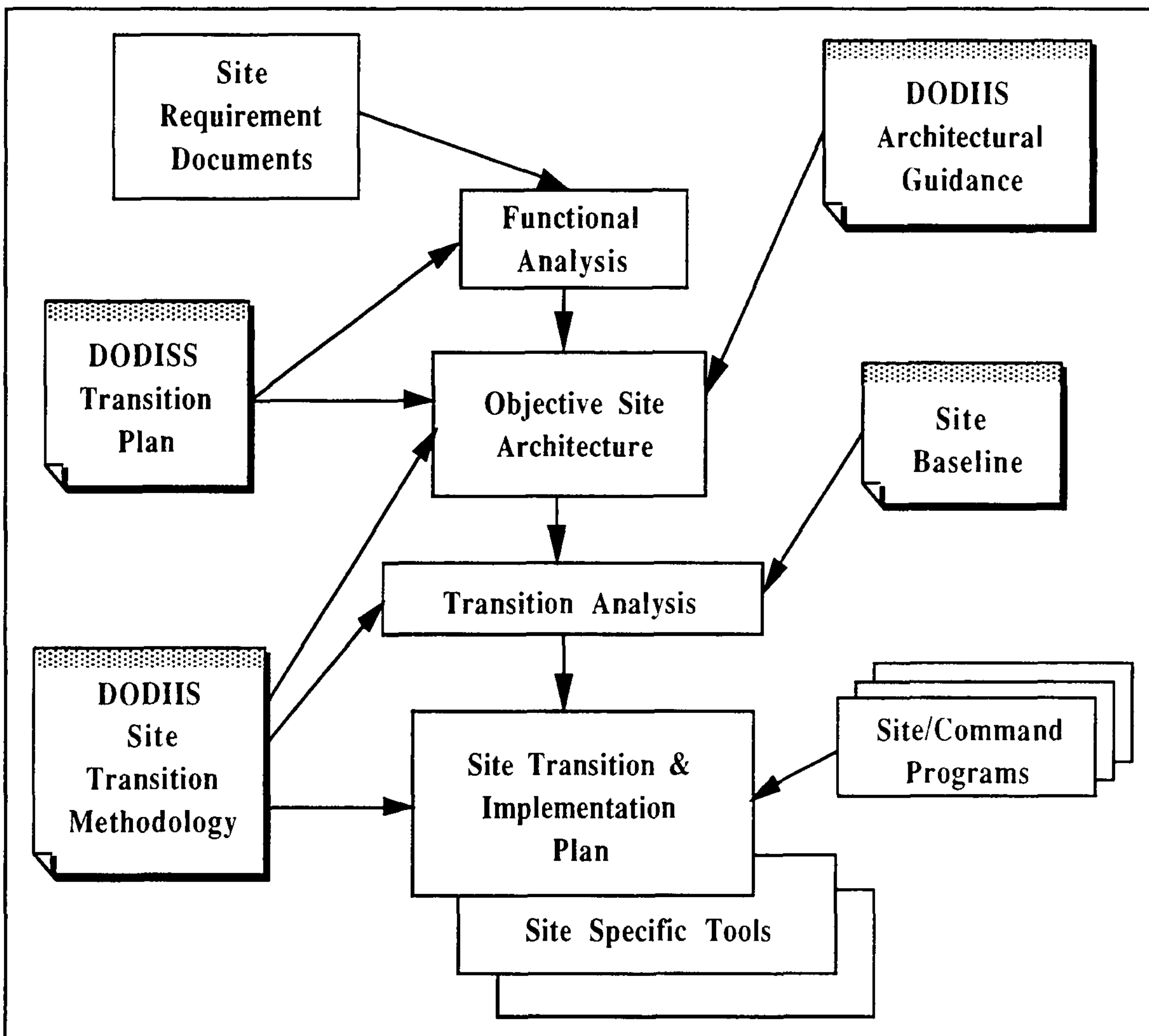

Figure 3: Overview of DODIIS Site Transition Methodology
[Ref. 10:p. 3-2]

The objective site architecture is identified based on analysis of the site mission, relationships with other sites, and the flow of data into and out of the site. The analysis identifies the specific intelligence functions that should be performed at the site and justifies the selection of specific standards and site unique intelligence applications. This process is in line with strategic IS planning practices previously introduced that attempt to link the business and IS plans of the organization. The analysis process is intended to identify the intelligence functions of the organizations and map these functions to appropriate IS applications. Figure 4 depicts this analysis methodology. Three sets of data--formal mission documentation, relationships between sites, and data flows between sites--are used in the analysis.

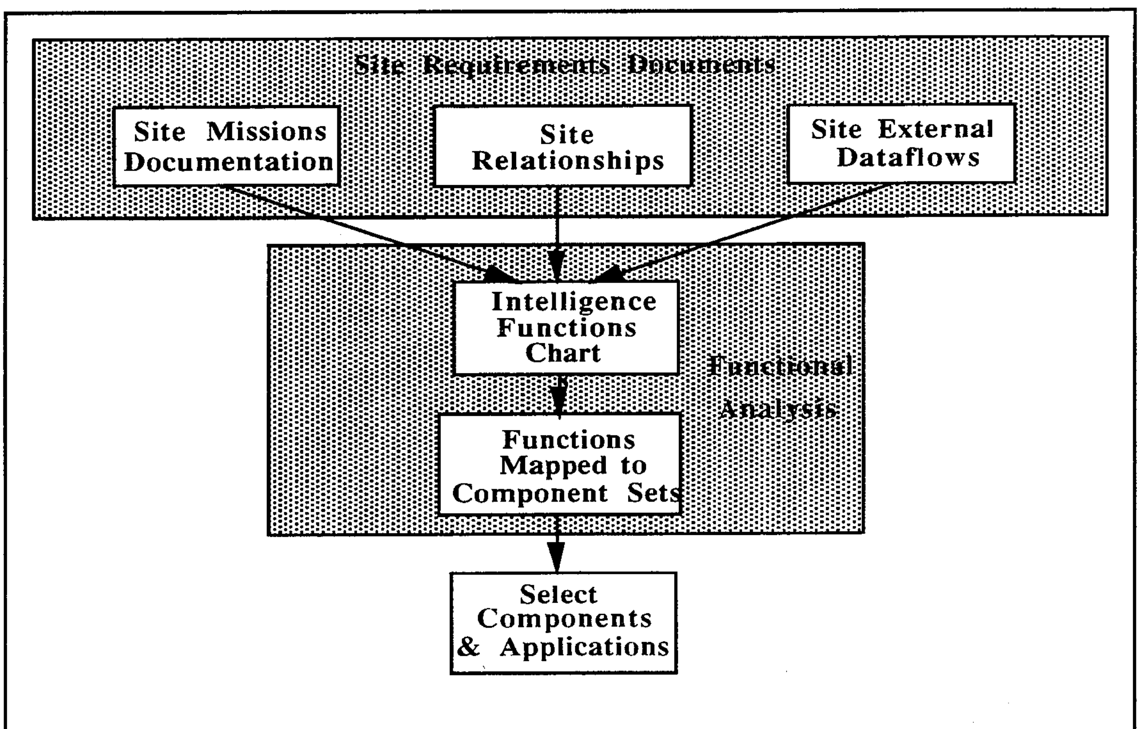

Figure 4: DODIIS Requirements Analysis Methodology [Ref. 10:p. 4-2]

Analysis of formal mission documentation typically reveals the general business plan of the organization. Further analysis of relationships with other sites (suppliers and customers) often will reveal additional capability requirements and provide insight regarding the performance of formally defined missions. The DODIIS site transition methodology provides a one page summary chart for recording these relationships. Figure 5 is a example for a "notional" intelligence site with tasking, evaluation, and support relationships between the sites described. This example uses a generic intelligence site with possible relationships to a Joint Task Force (JTF), the Defense Intelligence Agency (DIA), a Theater Joint Intelligence Center (JIC), as well as Tactical Users depicted.

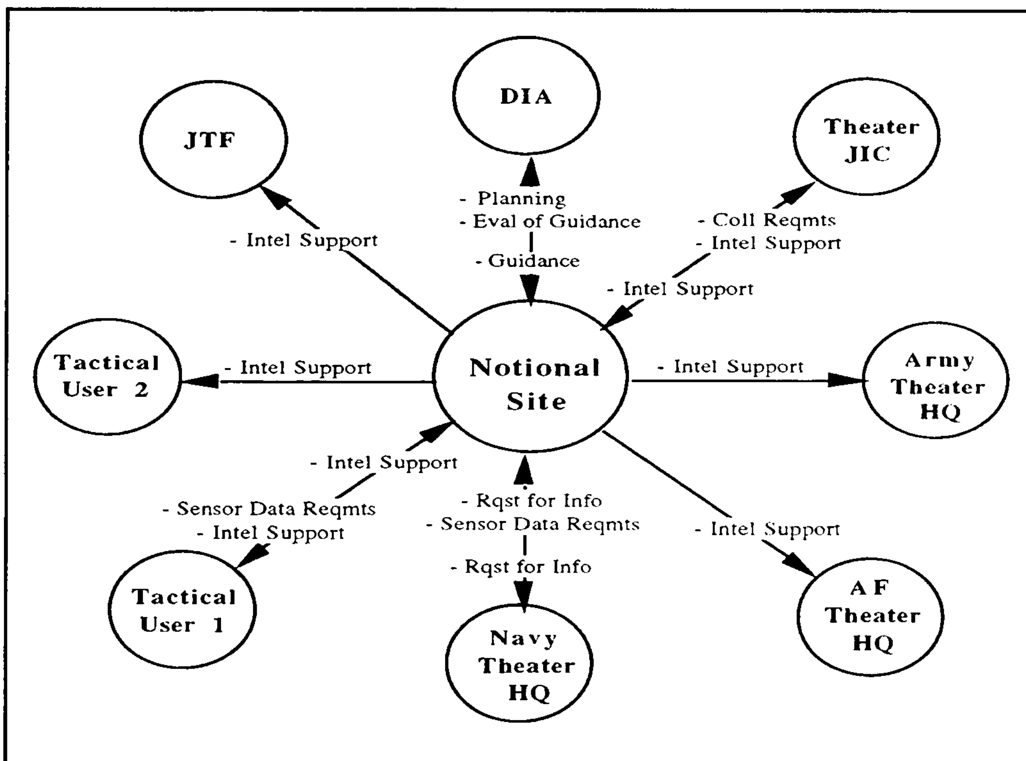

Figure 5: Example Intelligence Site Relationships [Ref. 10:p. 4-4]

After reviewing mission-related documentation and establishing external organizational relationships, the DODIIS Site Transition Methodology calls for further analysis to be conducted that identifies information requirements by considering data flow between sites. Data flows are also summarized on a one-page chart. The data flows show the source, destination , and type of intelligence data and products (services) flowing in and out of the site. The format is the same as the organizational chart, except that the arrow notations are used to indicate information flows instead of relationships. Figure 6 shows an example Data Flow chart for the same "notional" intelligence site.

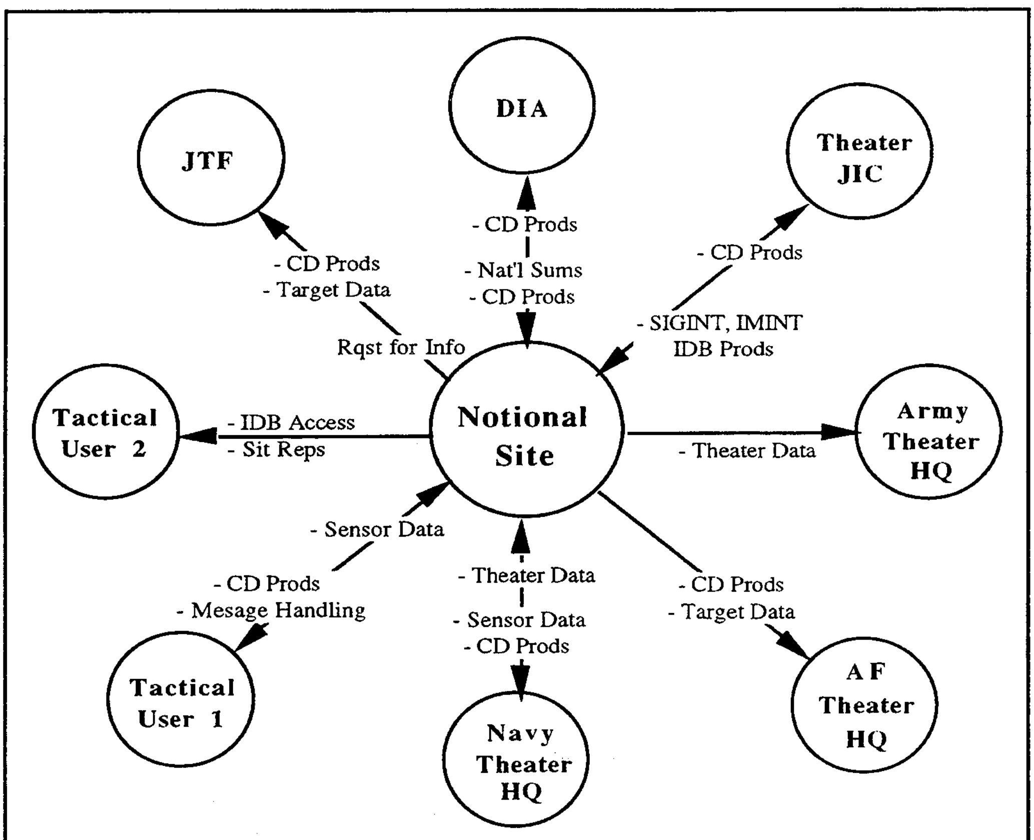

Figure 6: Example Intelligence Site Data Flows [Ref. 10:p. 4-6]

The organizational and data flow analysis provides the understanding required to develop the baseline and objective site architectures. An understanding of the information requirements is essential to the development of a strategic IS architecture that is aligned with organizational goals and critical business functions of the organization. The DODIIS methodology is specifically designed for intelligence organizations, but is consistent with previously reviewed strategic IS planning methodologies. In summary, the purpose of the DODIIS Site Transition Methodology is to provide guidance for:

- Developing site implementation of the standard DODIIS site architecture;
- Developing a site transition plan;
- Managing the transition using standard project management techniques.

E. INTEGRATING ARCHITECTURAL METHODOLOGIES

The architectural IS planning methodologies presented in this chapter offer a broad range of techniques which are intended to assist in the development of an IS plan that is strategically aligned with the critical business functions of the organization. Similar to all strategic IS planning guidelines, the architectural approaches offered by the TAFIM and DODIIS methodologies emphasize a structured approach that can be applied to both large and small organizations. The TAFIM SBA Planning Guide presents the step-by-step process. The DODIIS guidelines provide a complementary set of steps with application specifically useful for intelligence organizations.

This thesis in subsequent chapters will use an integrated approach to architectural IS planning that draws on the techniques presented in this chapter. Primarily, the methodology presented will follow the structured steps of the TAFIM SBA Planning process. These steps will form the structure and outline for addressing the architectural development issues at ONI. Additionally, the techniques offered by the DODIIS guidelines that are specifically useful for intelligence organizations will be used when applicable.

III. INITIATION AND ARCHITECTURE FRAMEWORK

A. INTRODUCTION

This chapter will begin the demonstration of the TAFIM SBA Planning process with application to the systems development efforts underway at ONI. As described in the SBA Planning guide, phase one is Initiation and Architecture Framework. Subsequent phases will be addressed in following chapters. As previously discussed, the entire planning process described in the SBA Planning Guide will not be attempted. However, the structure for this chapter will be similar to that envisioned for the *Architecture Framework Document* described in the SBA Planning Guide. As such, this chapter is intended to be direction-setting in nature. This chapter will be structured around the major deliverables described in the SBA Planning Guide:

- Enterprise Mission/Vision
- Strategic Drivers
- IT Principles
- Key Issues Impacting Architecture Development

B. ONI's ENTERPRISE MISSION / VISION

The following quote is taken from the ONI strategic planning document entitled *Strategic Planning for the Office of Naval Intelligence: Vision and Direction for the Future* promulgated in July 1992:

> ONI's ongoing intelligence role is now defined as providing basic and background maritime intelligence for the JICs; providing support to Department of the Navy RDT&E, acquisition, and training functions; providing maritime

> S&T and general military intelligence support to many branches of the Government; and support for certain unique national-level programs . . . [In this role] ONI is *the* national resource and center for excellence for maritime intelligence world-wide: services, analysis, special collection, training, and technical resources. [Ref. 11:pp. 2-11]

Subsequent to this initial planning document, the ONI leadership began a formal strategic planning process in mid-October 1992. ONI's mission and its vision statement were reaffirmed after carefully examining the environment within which ONI was to operate.

The early planning initiatives by ONI in 1992 led to the establishment of five "Key Issues" and associated accomplishments to be the focus for planning ONI's development over the succeeding five to seven years. These key strategic planning issues are shown in Table 2. All of these key issues will either directly or indirectly influence the strategic IS planning process at ONI.

TABLE 2: ONI'S KEY STRATEGIC PLANNING ISSUES [Ref. 12:pp. 3-4]

Key Issue 1. Customers
Key Accomplishment: With our customers, establish a clearly defined and accepted set of relationships, products, and services.
Key Issue 2. Workforce
Key Accomplishment: Create an atmosphere that promotes a motivated and capable workforce that clearly understands ONI goals and their role in supporting them.
Key Issue 3. Resource Planning
Key Accomplishment: Optimize resources to ensure the capability to carry out our responsibilities.
Key Issue 4. Demand-Pull
Key Accomplishment: Support a multi-media, demand-pull dissemination system.
Key Issue 5. National Maritime Intelligence Center
Key Accomplishment: Achieve a fully operational national maritime intelligence capability within the new facility.

Table 3 summarizes the primary missions for ONI. The emphasis in each of the four customer-oriented missions is on *services*, not *products*. In many cases, the *service* will be the acquisition of data collected by ONI assets or by other organizations, the analysis and fusion of that data, the addition of explanatory comments and information, the tailoring of the material for use by the customer, and its timely delivery on-demand to the customer. [Ref. 11:p. 13]

Finally, the ONI Strategic Plan calls for a change from the traditional production of:

> . . . a relatively fixed slate of information publications to providing demand-pull *services* to customers who can tailor their own *products* through querying a universally responsive, on-line database from any point on the globe. That is ONI's vision, one fully supported by the defense community, but one that will require careful and comprehensive planning, judicious expenditure of resources, and constant liaison between ONI and its customers to bring to reality. [Ref. 12:p. 3]

TABLE 3: ONI MISSIONS SUMMARY [Ref. 11:p. 12]

Mission 1 - Provide the Joint operating forces, via the Unified and Specified Commanders' JICs, with intelligence and resources for:

Naval ship and aircraft characteristics, capabilities, operating doctrine and tactics
Merchant ship information, locations, and tracks
Environmental and geophysical data
Tailored support for special collection and operations
Specialized tactical and operational analysis
Identification of threats, vulnerabilities, and proactive opportunities

Mission 2 - Provide the Department of the Navy with intelligence and services for:

Scientific and Technical Intelligence to support research, development, testing, operational evaluation and acquisition
Professional development and training intelligence specialists and officers
Requirements and planning, programming, budgeting for intelligence and related systems and personnel
Tailored support for special collection programs

Mission 3 - Provide National Security elements of the Government with maritime intelligence and support for:

Counterintelligence and security operations
Counterterrorism operations
Counterdrug operations
Nuclear and nonnuclear arms proliferation monitoring
Treaty and multilateral agreement verification
Strategic trade monitoring and global economic assessment
National intelligence estimates
Ocean resources and the maritime environment data collection

Mission 4 - Provide the Fleet and Fleet Marines with maritime intelligence for tactical training, rehearsal and preparation for:

Naval surface and undersea warfare
-- Cued by real world tactics, capabilities, and vulnerabilities of potential adversaries
Naval air warfare
-- Cued by realworld air defense systems and tactics, capabilities and vulnerabilities.
-- Incorporating air defense and air traffic control systems worldwide as they have been exported
Naval amphibious and strike power projection ashore
-- Cued by realworld coastal and interior environments and defenses
-- Incorporating air and land defense systems worldwide as they have been exported or developed

Special Mission: In addition ONI also must support certain national level programs.

C. STRATEGIC DRIVERS

1. Key Strategic IS Planning Initiatives

Recent C4I systems development within DoD has been guided by several key initiatives developed during the late 1980s and early 1990s. These initiatives have provided a vision for information management within DoD and directly influence current and future systems development efforts within the Navy and at ONI. These initiatives emphasize the common theme of providing timely and accurate information to the user, creating an interoperable information environment across DoD.

In order to understand and effectively evaluate critical C4I systems development decisions, these key policy initiatives must be examined. The guidance provided by these initiatives is reflected in recent C4I systems integration efforts within the Navy. This section will examine these initiatives and attempt to provide an understanding of the resulting current and future systems development trends.

a. DoD's Corporate Information Management (CIM)

Defense Management Review Decision (DMRD) 918 provided support for the Corporate Information Management (CIM) initiative administered by the Defense Information Systems Agency (DISA). CIM is a strategic management initiative intended to guide the evolution of the DoD enterprise by capturing the benefits of the information revolution. It emphasizes both a functional and technical management focus to achieve a combination of improved business processes and effective application of information technology across the functional areas of DoD. It is embodied in policies and programs, implementation guidance, and supporting resources, to help functional managers guide and implement changes to processes, data, and systems across the DoD. [Ref. 13:p. 1]

The management structure of CIM has four "pillars" that support improved Defense capabilities: common information systems; shared, standard data; re-engineered processes; and a computer and communications infrastructure. The overarching goal of CIM is to enable commanders of military forces and managers of support activities to achieve the highest degree of capability in their operations through the effective use of information applied in improved functional processes. The vision of this initiative provides for global end-to-end information connectivity among U.S. and allied forces. In this context, information is considered a critical mission capability and force multiplier for worldwide readiness, mobility, responsiveness, and operations. Joint interoperability and information integration on the battlefield is emphasized to result in significantly improved joint service and multinational operations. [Ref. 13:p. 3]

b. The Joint Staff's "C4I for the Warrior"

C4I for the Warrior is a concept for DoD information management first published by the Joint Chief's of Staff in 1992. It is clearly targeted at solving the C4I interoperability issues among the services. The intent is to provide an unifying C4I concept that will support the requirements of the joint force Warrior at the battlefield level, while remaining consistent with DoD policy and national security objectives. This focus is expressed by former Chairman, General Colin L. Powell, in the following statement:

> The C4I for the Warrior concept will give the battlefield commander access to all information needed to win in war and will provide the information when, where, and how the commander wants it. The C4I for the Warrior concept starts with the Warrior's requirements and provides a road map to reach the objective of a seamless, secure, interoperable global C4I network for the Warrior. [Ref. 14]

C4I for the Warrior is considered a seminal doctrine that is intended to guide the evolution of individual service C4I architectures into a broad Global Command and Control System (GCCS) [Ref. 15:p. 49]. The concept principles have been incorporated in the Joint Staff's GCCS program.

At the center of the C4I for the Warrior concept is the establishment of a global C4I capability that allows the Warrior to define the battle space and to "plug in" and "pull" timely, relevant information anytime, anyplace in the performance of any mission. The Warrior, by defining the battle space, determines the information to "pull" rather than have information "pushed" from various sources. The Warriors neither want nor need the cumulative knowledge of multiple sources dumped into their battle space information systems. They want only the specific information they need to win the fight; and they want it when they need it, where they need it, and in the form in which it will do them the most good. This demand pull concept provides the capability for the Warrior to poll the global C4I network for any desired information from any location, at any time. This is a key principle of the C4I for the Warrior concept and a guiding concept for future DoD and Navy C4I architecture development.

c. The Navy's Copernicus Architecture

The Copernicus Architecture is the current architectural guidance designed to restructure all Navy C4I systems. *The Copernicus Architecture, Phase 1: Requirements Definition*, published in 1991, provides both a new C4I architecture to replace the current

Navy system and a programmatic investment strategy to construct it over the next decade. It is intended to establish a vision of an overall C4I architecture for the Navy. [Ref. 16:p. 3-2]

The Copernicus Architecture is primarily a telecommunications system designed around a series of global information exchange systems ashore and tactical information exchange systems afloat. The architectural concept is based on four pillars: first, virtual global networks called Global Information Exchange Systems (GLOBIXS); second, metropolitan area networks called CINC Command Centers (CCC); third, tactical virtual nets called Tactical Data Information Exchange Systems (TADIXS); and fourth, interconnecting the previous systems to support the Tactical Command Center (TCC) afloat. In this concept, data can be forwarded from the shore based sensor-to-sensor infrastructure to the tactical commander's C2 infrastructure afloat. This new system has been designated Copernicus as it is centered on the tactical needs of the operator afloat. [Ref. 17:pp. 10-12]

A key concept of the Copernicus Architecture is the recognition of the Space and Electronic Warfare Commander (SEWC) as part of the Composite Warfare Commander (CWC) doctrine afloat. This action follows the establishment of SEW as a designated warfare area within the Navy by the CNO in 1989, which doctrinally assigned command and control (C2) functions to the SEW mission. In many ways, this early recognition of the importance of information management for the operational commander served as a building block for further DoD architecture development. The Copernicus goal of establishing a "common operating environment" now is considered part of the Defense Department's "C4I for the Warrior" initiative, which requires the Army, Navy, and Air

Force to develop, through a phased process, approaches to making their C4I data-transfer systems fully compatible for joint operations. [Ref. 15:p. 49]

d. Summary of Key Policy Initiatives

The policy initiatives reviewed in this section have provided the fundamental guidance for recent systems development throughout DoD and within the Navy. These initiatives present the common theme of support to the operational commander or Warrior through an integrated strategic information management infrastructure and the development of interoperable C4I systems. These initiatives present a consistent view of C4I from the afloat operational commander to the Unified CINCs crossing all DoD functional areas. The impact of these policy and strategy initiatives is reflected in recent C4I systems development efforts and has influenced the actual deployment and delivery of operational C4I systems to the field.

2. Key IS Development Directives

a. OSD Guidance for C4I Systems Development

Additional policy guidance has been incorporated into more recent national military planning strategy and DoD directives to reflect the goals of these key initiatives reviewed in the previous section. As a result, new systems are being development in line with joint doctrine. DoD Directive 4630.5 states, "That for the purposes of compatibility, interoperability, and integration, all C3I systems developed for use by US forces are considered to be for joint use." The National Military Strategy Document (NMSD) for FY 1994-1999 establishes C4I as the overarching C4 programming objective. The NMSD's reiterates the concepts. "Consistent with the 'C4I for the Warrior' plan, all Service- and

Agency-programmed systems must be compatible and interoperable to support joint and combined operation across the entire spectrum of conflict." [Ref. 18:p. 18]

DoD systems development efforts have recently been given further direction in order to programmatically achieve the goals of the strategic initiatives. The elimination of duplication and technical obsolescence among C4I systems currently in service across DoD prompted direction from Deputy Secretary of Defense Perry in a memorandum of October 13, 1993. This memo directed an accelerated process for selection of systems to be included in set of "migration" systems. It also directed all development and expenditure for "legacy" systems to be terminated within three years. In compliance with DoD initiatives, complete data standardization is also to be achieved throughout C4I systems within three years.

Further direction from Assistant Secretary of Defense Paige in a memorandum of December 20, 1993, provided minimum specific evaluation criteria for selecting C4I systems for migration. It is important to note, as stated in this memo, that "... the perspective of the war fighter must be maintained throughout the selection process." [Ref. 19] Additionally, guidance provided with this memo indicated that the loss of system functionality would not be considered as justification to delay the migration system selection process.

All of these directives are intended to guide C4I systems development in this era of declining human and financial resources, increasing requirements, and resultant compressing schedules. As these directives indicate, program managers must design, develop, procure, and support affordable systems necessary to meet Naval and joint C4I requirements in the face of these constraints.

b. DNI Guidance for ONI Systems Development

The key strategic initiatives and planning guidance provided will have a direct impact on ONI systems architecture development efforts. Many systems now used at ONI have been identified as legacy systems. Those systems may be dropped completely. The unique functionality of those legacy systems must be merged with a migration system if functionality is to be maintained and further supported.

In line with the current systems development environment within DoD, policy direction from the Director of Naval Intelligence (DNI) has stressed compatibility and interoperability of ONI systems with DoD-wide efforts. ONI's systems development efforts over the last decade have been supported by the Naval Command, Control, & Ocean Surveillance Center (NCCOSC), Research, Development, Tests, & Evaluation Division (NRaD), the Navy's lead C4I systems development agency. Given that the genesis of the new Global Command and Control System (GCCS) is the Joint Maritime Command Information System (JMCIS), the basis exists to implement within ONI a truly interoperable, open systems, C4I architecture that will support national, theater, and tactical customers. Recent development efforts at NRaD have been focused on design and implementation of a common architecture and structure that can accommodate unique ONI analytical requirements within the JMCIS framework. In a memorandum of September 10, 1993, the DNI directs that "... as a matter of policy, all ONI systems development will be accomplished in strict adherence with the JMCIS architecture and its established systems development procedures." [Ref. 2]

D. DEVELOPING ONI's IT PRINCIPLES

After reviewing ONI's strategic planning guidance, several key IT-related issues become apparent. Additional issues of concern have been obtained during personal interviews with key management and technical personnel at ONI and NRaD. It is the general goal of ONI to build an IS architecture that supports its customers and its own mission-critical functions with responsive data bases and on-line information services. This architecture development is to be accomplished consistent with DoD-wide IS architectural initiatives. These IT-related issues must be specifically addressed in the strategic IS planning process. They are essential to creating an IS plan that will support the strategic vision of ONI and will be reflected in its IT principles. The section provides a few suggested IT-principles to be used in ONI's architecture development effort. This is obviously not an exhaustive list, but is provided to demonstrate the concept of developing IT-principles to guide the architectural IS planning process.

1. Meta-Principles

Principle

Implement a demand-pull capability for ONI's intelligence dissemination.

Rationale

The ONI strategic vision calls for serving ". . . its customers in the most efficient and effective way possible." The emphasis is placed on identifying opportunities and developing new methodologies to accelerate change in the way intelligence is delivered. Traditional supplier-push systems, in which the intelligence producer creates and sends to the customer hard copy covering "everything the customer might need to know," must evolve, where warranted, to demand-pull systems, in which intelligence is provided "on demand" to the customer, tailored to a particular user's immediate requirements.

Implications

This concept will require ONI to transition from a document and database orientation to an information-based orientation, transforming itself from a document producer to an information service provider. This requires structuring intelligence in such a way that the customer is able to access any data, database, or information related to a general concept. Achieving a concept oriented demand-pull dissemination architecture will require an integrated concept of operations, adherence to standards, and systems interoperability at multiple levels. [Ref. 12:p. 25]

Principle

All ONI systems development will remain consistent with DoD-wide strategic IS initiatives.

Rationale

ONI's Strategic Plan specifically recognizes two IS architectural initiatives "... which [will] affect the way ONI will communicate with its operational customers." The vision, goals, and actions planned by ONI specific address for these two initiatives:

1. The Copernicus architecture, which calls for fundamental changes in the C3I architecture of the Navy, especially with respect to the development of a global C3I network.

2. The Corporate Information Management or CIM initiative, whereby all DoD databases will become interoperational through standardized formats, syntax, and semantics. [Ref. 11:p. 10]

Implications

As ONI systems exist now, and as they continue to move on-line, they must conform to the CIM Standards wherever possible. Where this is not possible, action must be taken to extend or modify CIM Standards to accommodate the particular needs of maritime intelligence and decisions made with regard to evolutionary compatibility with CIM. [Ref. 11:p. 22]

A driving concept of *Copernicus* is the emphasis on demand-pull data services as opposed to supply-push data production. This concept is in full accordance with ONI's goal to emphasize services vice products.

Principle

All ONI systems development will be accomplished in strict adherence with the JMCIS architecture and its established systems development procedures.

Rationale

This approach will enable ONI to provide maritime intelligence to a broad consumer base while affording the greatest degree of compatibility with Navy C4I systems converging under the JMCIS and GCCS architectures. JMCIS has been identified as the primary migration system for Navy C2. It will also allow for further support of unique ONI systems functionality that would otherwise be terminated as legacy systems are discontinued. It will allow ONI to maintain future IS expenditures within requisite fiscal boundaries. JMCIS provides an open systems architecture.

Implications

The functional requirements of legacy systems at ONI must be clearly identified for migration to the JMCIS architecture. Existing intelligence analysis applications will require integration into the JMCIS architecture and existing maritime data bases will require consolidation into a centralized system. This effort will constitute the development of ONI Intelligence Segment(s) within the JMCIS architecture.

Principle

All ONI systems development will be in consonance with DODIIS and TAFIM guidelines.

Rationale

In a January 1993 memorandum, then Director of Defense Information Mr. Paul Strassman stated that "The Technical Architecture Framework for Information Management (TAFIM) will serve as the single framework [to achieve integration] . . . and drive systems design, acquisition, and reuse throughout DoD." It was further directed that all new DoD information systems development and major modernization programs will use the TAFIM. TAFIM guidelines provide a structured approach to architectural IS planning that will ensure ONI systems achieve compatibility and interoperability with the broadest possible consumer base. The additional guidance provided through DODIIS will ensure ONI systems are aligned with those in the defense intelligence community.

Implications

The migration systems will form the foundation for future C4I architectures and are in consonance with DODIIS and the TAFIM standards. ONI efforts to conform with migration systems architectures, such as JMCIS, will ensure compliance.

2. Information Management

Principle

Create the National Maritime Intelligence Database (NMID).

Rationale

As the principal basis for the future functioning of ONI, the National Maritime Intelligence Database (NMID) is envisioned to be a multimedia, multilevel-secure, on-line, and on-demand service formed by the integration and extension of products, services, and data bases currently maintained at ONI. The NMID is intended to serve as the principal national information source for maritime intelligence and associated data including naval, merchant-marine, environmental, and scientific and technical information. [Ref. 11:p. 20]

Implications

Within the context of shifting the emphasis from *products* to *services*, the NMID will furnish three classes of services:

- On-line query-response services,
- Subscription services, using communications, electronic, optical, and paper media, and
- Outputs at ONI's own initiative when required, responding to interest profiles maintained by its customers.

NMID outputs, on consumer request, will be via query-response interaction directly with the NMID. The dissemination of standardized ONI data products will evolve into an on-demand system that incorporates broadcast and other broad dissemination via subscription services, extending the primary service of query-response alerting to any and all qualified consumers. Within this concept, the customer will clearly establish data requirements as well as directly influence analysis priorities and create interest profiles. [Ref. 11:pp. 20-21]

3. Application Management

Principle

Assure that local and external user requirements are satisfied with all systems development and acquisition processes, retaining the unique analytical functionality that current applications provide to ONI intelligence analysts.

Rationale

A primary concern is that the unique analytical capabilities of ONI that are currently supported with various information systems and applications, such as those specific to Civil Maritime Analysis, will continue to be supported in any new architecture. Migrating to a new architecture with new systems can mean trading systems maturity and reliable services of legacy systems for flexibility, openness, and unreliable services of new systems.

Implications

Again, the functional requirements of legacy systems at ONI must be clearly identified for migration to the new architecture. Existing intelligence analysis applications will require integration into the new architecture and existing maritime databases will require consolidation into a centralized system. Testing and validation will be critical to ensure functionality is maintained to an acceptable level.

4. Technology Management

Principle

ONI systems will migrate to an open systems, client/server environment.

Rationale

Client/Server is a flexible architecture that allows for integration of current systems in a distributed environment. Client/Server is argued to be the most logical means of realigning the IS architecture because it exploits the same perceived advantages of desktop computing, such as the reduced hardware and software costs, with increasingly powerful performance capabilities, while creating an environment that is responsive to the business needs of an organization. Other unique advantages include:

- System flexibility: The increasing standardization of protocols and "open systems" permits ad-hoc integration of disparate platforms. This environment is conducive to changing requirements for and allows the integration of old technology with new technology.
- Vendor independence: As more protocols and systems become standardized and open, users can select the system that provides the desired functionality.
- Reliability: In a client/server environment there is enough redundancy and machine independence to allow operations to continue. [Ref. 20:pp. 33-34]

Implications

This migration process is clearly underway at ONI. The inevitable implications of technological flexibility offered by the client/server environment has been increased architecture design and configuration management complexity. In the client/server environment, a network composed of mainframes and powerful desktop computers can all play a role. Configuration management and network management must be thoughtfully considered.

E. KEY ISSUES IMPACTING ARCHITECTURE DEVELOPMENT

This section reviews some of key findings previously presented to ONI in the thesis, *Downsizing Information Systems: Framing the Issues for the Office of Naval Intelligence*, completed by Lieutenant Peter Hutson in March 1994. These concerns have been commonly found in the commercial sector and are derived from corporate lessons learned. This direction-setting phase highlights issues relating to current IS architecture development efforts at ONI. These issues should be kept in mind as the architectural planning process progresses.

1. Organizational Considerations

- *An understanding of business needs is critical.* IT can only be a strategic asset to the extent that it supports the corporate strategy. Analysis of critical success factors in strategic IS planning may serve as an essential first step.

- *Top management support is an essential prerequisite.* It is an absolute necessity to the success of the effort that top corporate officials have "bought off" on the idea. Architectural IS planning must be part of the general strategic planning process.

- *Resistance to change should be anticipated and managed.* IS architectural change will provoke resistance. Proactive steps that facilitate communications and understanding throughout the organization must be taken to counter potentially negative reactions.

2. Architectural and Technical Considerations

- *Migration strategy is a critical decision.* Organizations need to decide to either (1) grow with their traditional mainframes, (2) fade out the mainframe while preparing replacement systems, or (3) kill the mainframe as quickly as possible. Commitment to a global strategy should help guide other decisions. Determining the optimal time to change, as well as the rate of change, should also be considered when selecting a migration strategy.

- *Downsizing and migration decisions can mean trading systems maturity and integrated services of legacy systems for flexibility, openness, and unintegrated services of distributed systems.* Despite their proprietary nature and expense, many corporations are unwilling to move mission-critical systems to an unproven, immature desktop environment.

- *Throughput capabilities remain a major strength of the mainframe.* The mainframe has been optimized to support high volume and complex data management with large bandwidth and the ability to manage multiple complex tasks. The most advanced and developed desktop systems are just beginning to compete with the mainframe in this area.

3. Cost Considerations

- *Cost/Benefit analysis must include conversion costs and costs of operating in the new environment.* Often the costs associated with conversion are overshadowed by the promises of cost savings in a new environment. Up-front conversion costs to distributed systems can represent a sizable investment.

IV. BASELINE CHARACTERIZATION

A. INTRODUCTION

This chapter continues the structured approach to architecture development as presented in the TAFIM SBA Planning Guide with phase two, the baseline characterization. The purpose of this phase is to determine the organization's current IS environment and create a report that characterizes the existing architecture of the enterprise. "A clear view of the existing IT architecture allows identification of opportunities for change. . ." [Ref. 7:Vol. 4,p. 3-1]

The term "characterization" is used because the data gathering and analysis are not exhaustive. It is not necessary, nor is it desirable, to expend the time and effort to document every detail of the current architecture. Only enough detail is gathered to allow informed decisions to be made with regard to the desired target architecture. The SBA Planning Guide emphasizes a "fast path" approach to the baseline. It recommends ". . . a generic baseline versus a detailed specific baseline." [Ref. 7:Vol. 4,p. 3-1] It suggests as a rule of thumb, that ". . . 80 percent of the information used in an architecture design activity derives from 20 percent of the data collected." [Ref. 7:Vol. 4,p. 3-2] Figure 7 illustrates the data collection dilemma indicating the inefficiency of spending time collecting the last 20 percent of the data when 80 percent is sufficiently accurate to characterize the current environment.

As described in the SBA Planning Guide, the baseline characterization is intended to produce a high-level description of the existing architecture along four key dimensions, or views: work, information, applications, and technology. This chapter and the baseline

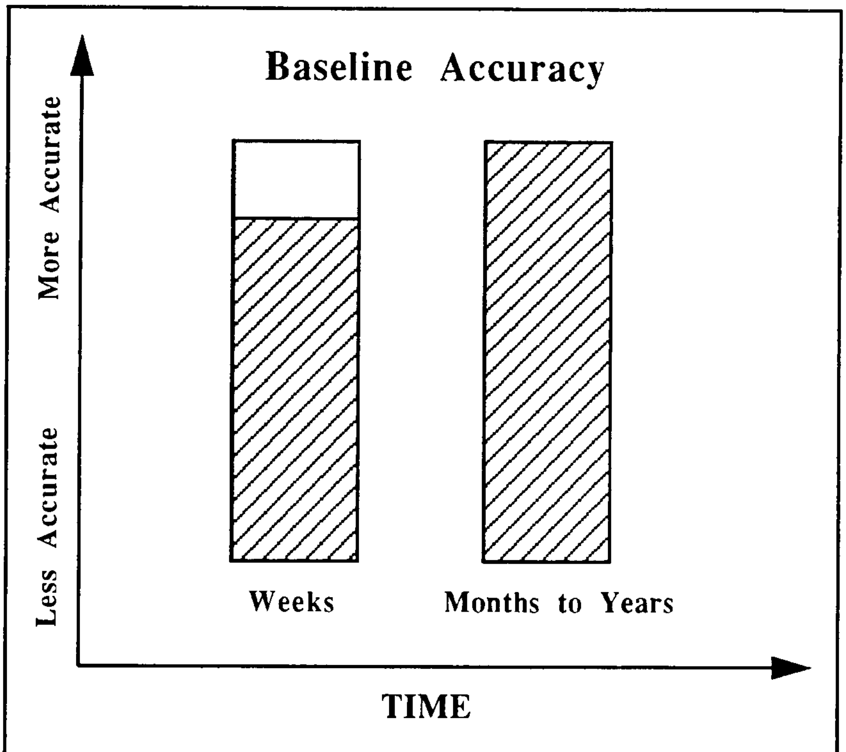

Figure 7: The Data Collection Payoff
[Ref. 7:Vol. 4,p. 3-2]

characterization presented will be structured around these four views:

- Work Organization View
- Information View
- Application View
- Technology View

B. WORK ORGANIZATION VIEW

As described in the SBA Planning Guide, the baseline inventory includes a characterization of all the business functions and the key processes that support the missions of the organization. The work organization view follows from the initiation and architectural framework phase by linking the specific missions of the organization to the supporting business functions. Similarly, the characterization of key processes follows the requirements analysis methodology outlined in the DODIIS Site Architecture guidance.

1. Organizational Structure

The physical work structure of an organization often does not accurately represent the actual business functions performed. Examining a hierarchical structure chart or line diagram provides an view of how the people and work groups are organized for management purposes. Examining the work group structure of an organization can provide a first glance understanding of the organization, but it does not reveal the business functions and key processes performed by the organization as a whole, which often cut across organizational boundaries. A broader functional analysis is required to characterize the work organization view in terms of information requirements for identification of the IS services required to support critical business functions.

The Intelligence Directorate (ONI-2) performs a broad range of substantive intelligence analysis functions. These functions include scientific and technical analysis as well as general military intelligence analysis. Intelligence production supports naval missions and functions to include:

- strategic commerce, seaborne weapons transfers, and embargoes;
- integrated regional naval threat analysis and support to the National Intelligence Estimate (NIE) process;
- surface and coastal warfare threat analysis and dissemination;

- air, electronic, and strike warfare threat analysis and dissemination;
- undersea warfare analysis and evaluation of vulnerabilities.

Figure 8 depicts the organizational chart of ONI-2 reflecting these mission areas.

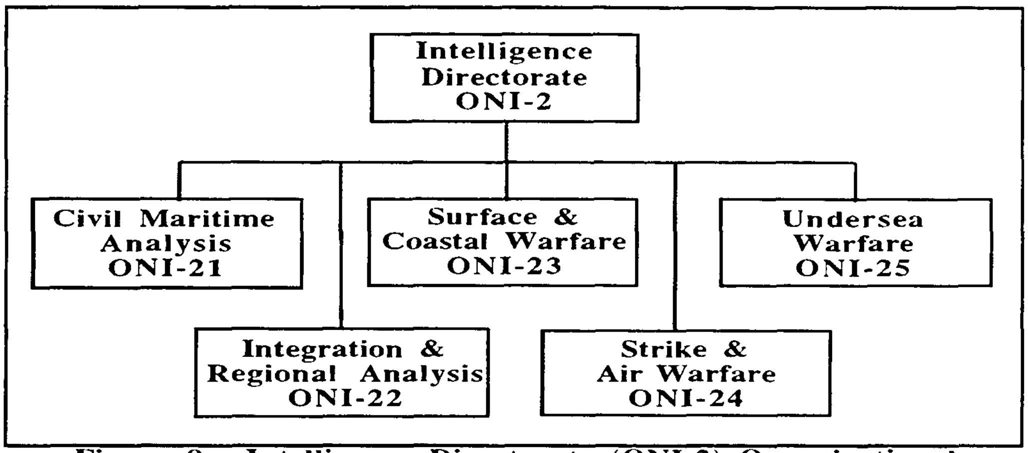

Figure 8: Intelligence Directorate (ONI-2) Organizational Chart

2. Business Functions

The Civil Maritime Analysis Department (ONI-21) focuses its analytical efforts primarily on the non-military use of the sea. This focus includes maintaining current and historical information concerning the characteristics, capabilities, disposition, operations, control, trade patterns, and cargo of all-flag merchant, fishing, and research vessels. This information supports analysis related specifically to seaborne arms transfers, embargo or sanctions monitoring, counter-drug support, strategic trade monitoring, international smuggling, control of illegal immigration, seaborne terrorism, and piracy.

The Integration and Regional Analysis Department (ONI-22) focuses its analytical efforts primarily on specific threat country or theater strategic issues. The analysis typically addresses issues that impact overall force structures and multiple warfare areas. In this capacity, ONI-22 provides coordination or support for issues of common interest to the Intelligence Directorate (ONI-2) as a whole. Analytical functions of this department specifically include assessments of foreign naval-related technologies, monitoring of global weapons development infrastructures, supporting arms-control negotiations, monitoring regional military-political and economic developments, and analysis of operational employment of foreign strategic forces where the interests of U.S. Naval forces are involved. ONI-22 also provides a 24-hour watch that includes watch personnel in the National Military Joint Intelligence Center (NMJIC) and Naval Command Center providing timely assessments of significant foreign-maritime developments to the Joint Chiefs of Staff, the Secretary of the Navy, the Chief of Naval Operations, the Director of Naval Intelligence, and other key decision makers.

The Surface and Coastal Warfare Department (ONI-23) focuses analysis specifically on hostile foreign naval operations that pose a potential near-term threat to U.S. Naval surface operations. The analysis is related to mine warfare, coastal defenses, anti-landing capabilities, and anti-ship capabilities of foreign navies. ONI-23's intelligence reporting and dissemination directly supports U.S. Naval forces as well as the national and defense intelligence process. Additionally, support is provided to training and weapons acquisition programs relying on foreign naval capabilities and performance information.

The Strike and Air Warfare Department (ONI-24) focuses analysis specifically on foreign air and space operations including tactics, training, and readiness. Threat analysis is conducted to determine capabilities, performance, and potential vulnerabilities of foreign strike and air warfare platforms. Likewise, the Undersea Warfare Department (ONI-25) focuses its analytical efforts specifically on foreign naval submarine and anti-submarine warfare operations including tactics, training, and readiness. Threat analysis is conducted to determine capabilities, performance, and potential vulnerabilities of foreign undersea warfare platforms and systems. Reporting and dissemination directly support U.S. Naval forces and various national and military agencies.

Examining the organizational structure of ONI-2 provides a general understanding of the mission areas while a more thorough examination reveals the business functions that support the missions areas. A functional analysis, independent of mission area, provides a better understanding of the roles and processes that are common across the physical organization. It is these roles and key processes that identify and best characterize the critical business functions of the organization. Table 4 below provides a summary of the maritime intelligence roles supported by the analytical functions performed within ONI-2.

3. Key Processes

An analysis of the primary missions areas and supporting business functions performed within ONI-2 reveals a few key processes that are common among each work group regardless of the organizational structure. Similar to most intelligence organizations, the key processes performed within ONI-2 are directly related to the basic processes performed in the generic intelligence process known as the intelligence cycle. The intelligence cycle refers to the sequence of steps or phases by which data is gathered and

TABLE 4: ONI MARITIME INTELLIGENCE ROLES [Ref. 11:p. 15]

Combat Support	Planning, Programming, Budgeting
Indications and Warning	Counterintelligence and Security
Special Operations	Counterterrorism
Special Maritime Collection	Counterdrug
Tactical Analysis	Nuclear Proliferation Control
Threat and Opportunities Analysis	Treat Verification and Arms Control
Tactics Development and Evaluation	Strategic Trade and Economic Intel
Training - Combat	Multilateral Agreements
Training - Military and Civilian	Intelligence Estimates
Training - Professional Development	Ocean Services and Resources
RDT & E and Acquisition	Ocean Environment

transformed into meaningful information that is then made available to users or consumers. This cycle consists of three key processes: (1) collection, (2) production, and (3) dissemination.

The collection phase deals with the planning and preparation required for obtaining and forwarding selected data and information about a specific objective. Its focus is the acquisition of data for further processing. During the collection phase, decisions regarding the selection, allocation, and use of operational and intelligence sources are made to obtain the required information. Collection provides the essential data for the intelligence process. The data derived in the collection phase is evaluated in the production phase.

The production phase involves the conversion of collected data into a form suitable for the user. This conversion process involves manipulating the collected data through integration, analysis, evaluation, and interpretation into an intelligence product. This process of converting collected data into an intelligence product is the primary process common to all work groups within ONI-2 regardless of mission area. The analysis performed at the production phase is the key business function of the organization and requires direct support from automated information systems and their applications. "The intelligence analyst, working with raw information collected from a variety of sources, selects, verifies, compares, infers, interprets, and acts upon available information and intelligence to produce a usable end product." [Ref. 21:p. 7-1]

The final phase in the intelligence cycle is dissemination of the refined intelligence product or service. This phase specifically involves the conveyance of the intelligence product or service to the consumer or user. It is pointless to collect data and to process it into meaningful intelligence if it does not reach the proper consumer at the proper time. Dissemination can take on many forms. It covers a broad spectrum ranging from a brief telephone response to the transfer of large volumes of detailed and comprehensive intelligence documents. Effective intelligence dissemination requires (1) that the consumers having the need to know receive the information, (2) that delivery of the information is timely, and (3) that the information reaches the consumer in an appropriate form. Automated information systems have significantly impacted the means of dissemination and provide direct transmission of the information to the end user. [Ref. 21:p. 8-1]

The key processes in the intelligence cycle are commonly performed within each ONI-2 department regardless of the analytical focus of the work group or division. Each intelligence product or service can usually be traced back to its origin through the individual phases in the cycle. As a whole, however, the cycle can be viewed as having no beginning or end point. Instead, the intelligence cycle is an ongoing series of key processes with all the steps typically occurring concurrently.

C. INFORMATION VIEW

The information view of the current architecture is intended to provide a high-level understanding of the information needed to perform the work of the enterprise. The information view focuses on the data being managed in support of work groups and external customers. Models provide an understanding of the relationships with customers and the mission critical data flows to and from the customers. As stated in the ONI Strategic Planning document, "The essence of our excellence lies in this synergy of human and technical resources and in the application of naval expertise to convert data to information." [Ref. 11:p. 11]

1. Organizational Relationships

The business functions performed by ONI-2 are in direct response and support to ONI's broad customer base. Analysis of intelligence relationships with these external customers will reveal additional capability requirements and provides insight regarding the performance of the formally defined missions. These organizational relationships are often not defined formally, and must be identified and recorded as part of the architectural effort. The DODIIS architectural guidance provides a one-page summary chart for recording these relationships.

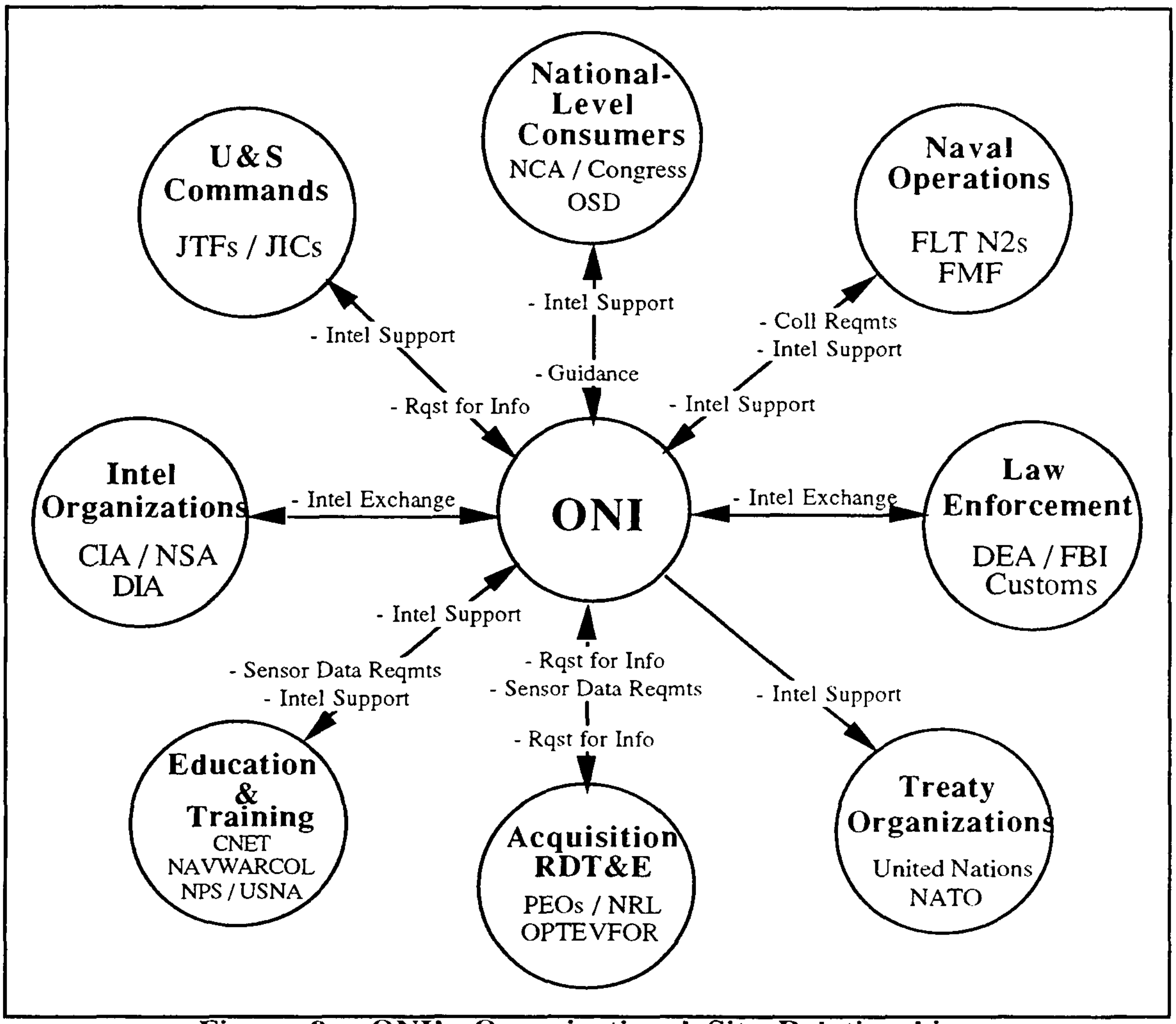

Figure 9: ONI's Organizational Site Relationships

Figure 9 shows the general relationships with ONI's primary customers with tasking, evaluation, and support relationships depicted between sites. The example, Figure 9, shows the following:

- Guidance from the National Command Authority (NCA), Congress, and the Office of the Secretary of Defense (OSD) concerning organization, funding, and responsibilities with intelligence support provided to key decision makers.

- Intelligence support provided directly to naval forces with additional collection requirements established. This includes direct support to fleet intelligence officers (FLT N2s and components of the Fleet Marine Forces (FMF).

- Cooperative agreements with law enforcement agencies to exchange information related to seaborne transfers of illegal cargoes. Agencies include the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI), and U.S. Customs Agency.

- Intelligence support provided to treaty organizations related to international agreements such as arms control or sanctions enforcement, including the United Nations and the North Atlantic Treaty Organization (NATO).

- Requests for information from organizations involved in weapons and defense systems acquisition and evaluations such as program executive officers (PEOs), research laboratories such as the Naval Research Laboratory (NRL), and weapons testing entities such as the Navy's Operational Test and Evaluation Force (OPTEVFOR).

- Analysis and support provided to educational and training commands such as the Naval War College (NAVWARCOL), the Naval Postgraduate School (NPS), and the U.S. Naval Academy (USNA). Analysis and wargaming efforts of these units provide ONI with additional analytical intelligence support.

- Intelligence exchanges and analysis efforts with other intelligence organizations such as the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Defense Intelligence (DIA) for example.

- A primary customer, the Unified and Specified Commands with their Joint Task Forces and the supporting Joint Intelligence Centers (JICs) that establishes intelligence requirements through requests for information and are provided with direct intelligence support from ONI.

2. External Data Flows

The final area of analysis for presenting the work organization view is external data flow analysis. Data flow analysis will indicate support to other sites that is not necessarily mission-specific. It also identifies required capabilities to accept data from other sites. Similar to the one-page chart used to summarize external relationships, Figure 10 summarizes the data flows using the DODIIS architectural guidelines. The format is the same as the organizational chart, except that the arrow notations are used to indicate example data information flows instead of relationships. For example, Figure 10 shows the type or form of data transfered between sites such as:

- Intelligence estimates provided to national-level consumers.
- Threat assessments provided to naval operational forces.
- Counter-Drug products exchanged with law enforcement agencies.
- Arms transfer data provided to treaty organizations.
- Specific weapons performance data provided to the research and acquisition community.
- Platform capability and characteristics data supporting education and training.
- Sensor data, such as Signals Intelligence (SIGINT), received from other intelligence agencies.

- And, requests for information received from the major joint commands that are then provided with specific targeting data, for example.

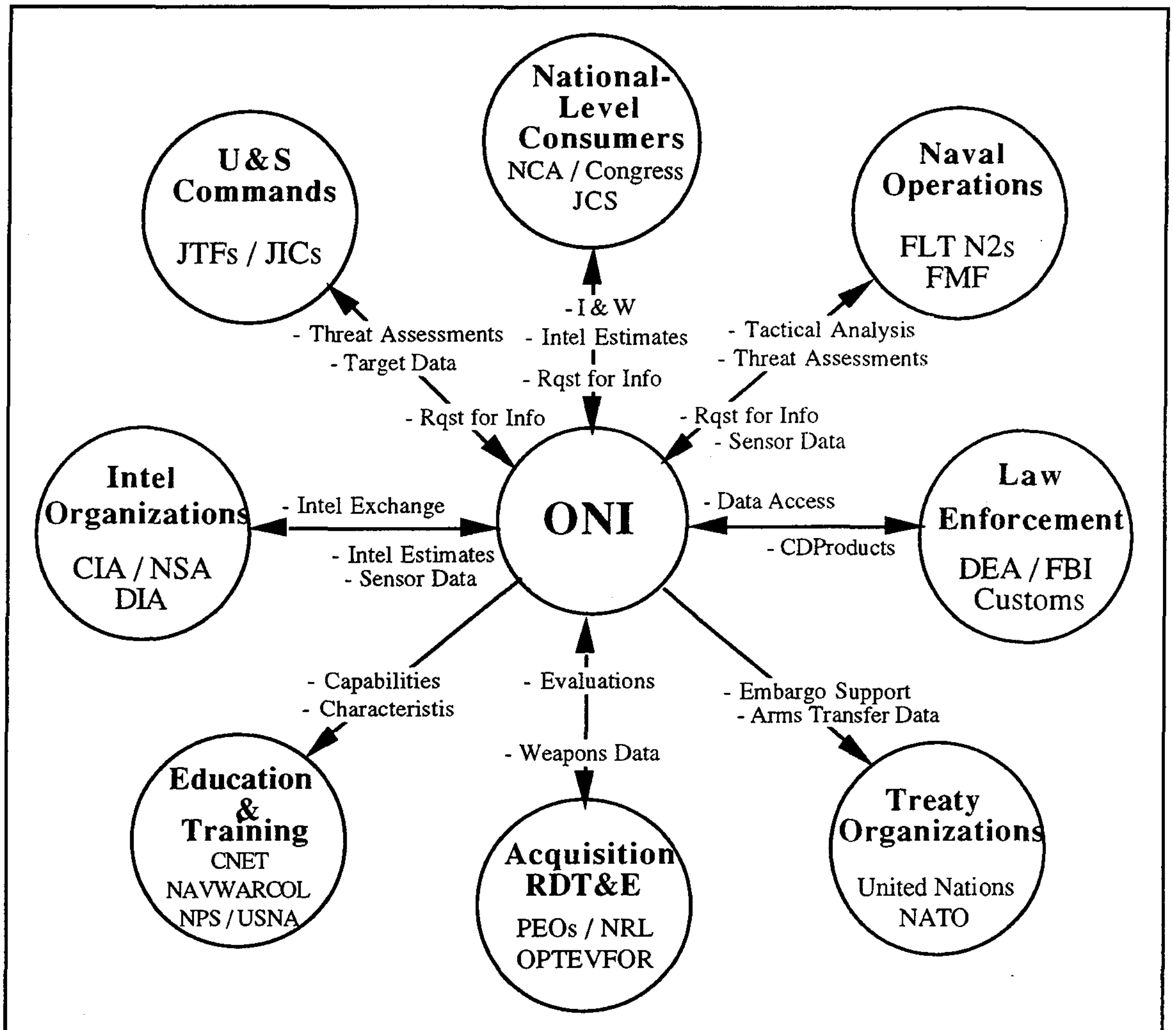

Figure 10: ONI Example External Data Flows

The organizational site relationships and corresponding data flows can take on many different forms, with only a few mentioned here. These relationships are depicted to characterize the type of information exchanges that must be supported by the intelligence applications within an automated information system. The processes involved with each relationship rely on information systems and specific applications with unique functionality. These applications will be discussed in the application view of this baseline characterization.

D. APPLICATION VIEW

The application view of the baseline describes the current applications, systems, and databases that directly support the mission-critical functions described in the work and information views. This view describes the high-level scope and interfaces among applications. The applications are described in terms of functionality and technical system components required. These systems currently support intelligence analysts within the Intelligence Directorate (ONI-2).

1. Automated Merchant Identification Ship System (AMIDSHIPS)

Functional Description: The AMIDSHIPS system provides automated capabilities for accessing ONI's civil maritime database of approximately 500,000 merchant ship photographs, plans, and drawings. It provides capability to input and annotate softcopy images which are stored on optical disks. It supports analyst database retrieval based on known ship characteristics. The images are identified by matching characteristics using a subset of the Naval Intelligence Database (NID) containing Merchant Ship Characteristics (MSC) data.

System Components: AMIDSHIPS is a workstation network based system hosted on SUN workstations including SUN 4/690 (server), 4/670 (server), 4/370, and Sparc 2. The operating system is SUN OS 4.1.4. The AMIDSHIPS application software is contractor developed with Sybase DBMS.

2. Collection Requirements Management Application (CRMA)

Functional Description: The CRMA system provides automated capabilities for centralized management of intelligence collection requirements, resulting products, and evaluations of Intelligence Information Reports (IIR) from DIA and the Navy. It provides tools to model collection systems, manage tasking requirements, predict availability of assets, and to store and recall reference data. The CRMA is a DODIIS core product.

System Components: CRMA is a network based system hosted on workstations including SUN 4/690 (server), SUN Sparc 2, SUN Sparc 10, and TAC-3. The operating system is SUN OS 4.1.3. The CRMA application software is government developed with Sybase DBMS.

3. Joint Maritime Information Element (JMIE)

Functional Description: The JMIE system provides a composite, multi-agency library of maritime data from multiple sources including open source, national foreign intelligence, and law enforcement agencies. Information on merchant shipping includes movement data, ship characteristics, port data, and organizational information. Seventeen U.S. Government agencies operate JMIE workstations at 33 different sites worldwide.

System Components: JMIE is a PC workstation-based system connected via DSNET1 or commercial phone lines (STU-III) to an IBM 4381 mainframe host located at the U.S. Coast Guard Operations Center in Martinsburg, West Virginia. The JMIE database interfaces with SeaWatch III and the Merchant Ship Characteristics (MSC) Database.

4. Merchant Ship Characteristics (MSC) Database

Functional Description: The MSC Database provides automated capability for the analysis of merchant ship characteristics throughout the life of the vessel in support of civil maritime analysis. It provides data base management capabilities for storage and retrieval of characteristics and performance data on merchant ships such as length, speed, displacement, etc. The MSC Database provides baseline data to several other systems directly or via magnetic tape including SeaWatch III, Naval Intelligence Database (NID), the Joint Maritime Information Element (JMIE), and AMIDSHIPS.

System Components: The MSC Database is hosted on a VAX 6410 supporting a network of approximately 62 PCs. The operating systems are VAX VMS 5.5 and MS-DOS. The MSC application software is contractor developed (MSC 1.0) with Oracle 6.0 DBMS.

5. Merchant Watch (MerWatch)

Functional Description: The MerWatch system provides tools supporting civil maritime analysis. This includes tools to generate merchant shipping related intelligence products with information on ports, cargo, ship movement, and organizations. The MerWatch software architecture represents a deliberate attempt to integrate existing civil maritime analysis functionality and databases into a single DODIIS-compliant system. MerWatch interfaces with the SeaWatch, MSC, and AMIDSHIPS databases.

System Components: MerWatch is a network-based system hosted on workstations including SUN 690MP (server), SUN Sparc 10 (42), SUN IPX (4). The operating system is SUN OS 4.1.3. The MerWatch application software is government developed (MerWatch D) with supporting commercial applications including Aster*x 2.1 AND ELT/2000 2.3. Oracle 6.0 is the DBMS.

6. Naval Intelligence Database (NID)

Functional Description: The NID provides automated capability for analysis of performance and characteristics data on threat platforms and the production of threat assessments and other publications. It also rovides database management capabilities for storing, retrieving, and analyzing threat characteristics data. The NID incorporates the MSC database.

System Components: The NID is hosted on a DEC ALPHA 7610 supporting various workstations including SUN, HP, MAC, PCs. The operating system is OpenVMS. The NID application software is contractor developed (NID 2.0) with Oracle 7.0 DBMS.

7. SeaView

Functional Description: The SeaView system provides analysts with state-of-the-art tools to create intelligence products by accessing, manipulating, and graphically displaying ocean surveillance information (from the SeaWatch III database). It provides capabilities to retrieve, sort, manipulate, and compare information from various data bases, as well as create colored maps and graphical displays with multi-dimensional views of the data.

System Components: SeaView is a network-based system hosted on approximately 30 workstations including the SUN 4 Sparc family. The operating system is SUN OS 4.1.3. The SeaView application software is contractor developed with SeaView/Sunshine 5.0.2. providing access to several external databases via DSNET3, in addition to SeaWatch III access.

8. SeaWatch III

Functional Description: The SeaWatch III system serves as ONI's central data processing system for ocean surveillance data. It provides automated capability to store, retrieve, and disseminate ocean surveillance data in support to civil maritime analysis. The database supports several applications and is support by the MSC database. The system receives reporting data from various sources. Primary capabilities and functions include message format input and output processing, automatic track correlation and association, data retrieval and manipulation, and a wide range of analytical, service, and administrative tools.

Capable of processing inputs from multiple data sources, SeaWatch receives an approximately 40,000 ship position reports per day. Over four million position reports are stored per year. SeaWatch constitutes the sole national resource for current and archival storage of merchant ship movement reports as well as the national archive for threat naval fleet movement data.

System Components: SeaWatch III is hosted on an IBM 3090 mainframe processor and Model 204 (v 2.2) database. It provides on-line support to over 100 analysts on both SUN 4 series workstations and PCs. The operating systems include the

MVS/XA, SUN OS 4.1.1, and MS-DOS. The SeaWatch III application software (v 1.5) is contractor developed.

E. TECHNOLOGY VIEW

1. General Description

The technology view of the current baseline architecture provides a general description of the major components of the computer processing and communications environment. The ONI Local Area Network (LAN) system is complex and serves over 2,000 intelligence analysts and support personnel. The system has grown over the years from a variety of self-contained, largely single-function users with their own separate and isolated LAN systems in two separate buildings, to a large complex of networked intelligence analysts and support personnel on a single, very large system located in a modern facility known as the National Maritime Intelligence Center (NMIC). The NMIC building is equipped with a Fiber Distributed Data Interface (FDDI) backbone supporting two primary internal network systems, the General Service (GENSER) LAN system, and the Sensitive Compartmented Information (SCI) LAN system. The NMIC is configured with fiber optic cabling to support these LAN systems. Ethernet (Transmission Control Protocol/Internet Protocol - TCP/IP) connectivity is provided to the backbone supporting the various systems and workgroup requirements.

2. General Service (GENSER) System

The General Services (GENSER) LAN System, which is used for transmission and receipt of collaterally classified information (i.e., Confidential and Secret data), is composed of the Joint Message Processing System (JMPS), a Vax-based host system which supports GENSER-level message and data traffic flow, and an Ethernet LAN system which supports ONI's requirements to have GENSER message traffic available to the analyst workstations from both the Automatic Digital Network (AUTODIN) and the Defense Secure Network (DSNET1). The GENSER LAN system supports the AMIDSHIPS and JMIE systems and the MSC database.

3. Sensitive Compartmented Information (SCI) System

The Sensitive Compartmented Information (SCI) LAN system supports the requirements for transmission and receipt of more highly classified information. The SCI LAN system supports the AMIDSHIPS, CRMA, MerWatch, SeaView, SeaWatch III systems and NID database. The SCI LAN provides analysts access to the Defense Secure Network (DSNET3).

4. The SeaWatch III System

The SeaWatch III system is an IBM mainframe-based system interfaced to the backbone via to the Ethernet network. The system retains its IBM Systems Network Architecture (SNA) and uses converters to interface the IBM mainframe (an IBM 3090) to the Ethernet network segment. The Seawatch III system has approximately 20 SUN workstations for analyst access, with many others gaining limited functionality access on PCs. Approximately 130 analysts have access to the system; however, there are generally no more than 20 to 25 people on the system at any one time. [Ref. 22:p. 8]

5. Automated Message Handling System (AMHS)

The current ONI Automated Message Handling System (AMHS) is designed to automatically receive and distribute incoming record message traffic to the users' workstations and to transmit via AUTODIN.

V. THE TARGET ARCHITECTURE

A. INTRODUCTION

This chapter presents a target architecture to guide systems development and evolution at ONI. This chapter specifically addresses the Joint Maritime Command Information System (JMCIS) architecture. A thorough understanding of the JMCIS architecture is essential to guide the architecture development efforts at ONI. As the current state of US Navy C4I systems, JMCIS represents a systems architecture that has evolved over the last decade, incorporating the functionality and objectives of multiple systems. This chapter presents this evolution to provide a background understanding of the current architecture. Finally, this chapter will present the specific application of the JMCIS architecture concepts to ONI system requirements and ongoing development efforts.

B. EVOLUTION OF U.S. NAVY C4I SYSTEMS ARCHITECTURE

1. Joint Operational Tactical System (JOTS)

The Joint Operational Tactical System (JOTS) began as a prototyping effort that was first deployed aboard ship in the early 1980s. This system provided the operational commander with the first integrated display of data for decision support purposes. System functionality eventually included track management, track analysis, environment prediction, and a variety of tactical overlays and Tactical Decision Aids (TDAs). JOTS was capable of receiving various data and message input such as Link 11, Link 14, Tactical Data Information Exchange System (TADIXS-A), Officer-in-Tactical-Command Information

Exchange System (OTCIXS), High Interest Track (HIT) Broadcasts, and U.S. Message Text Format (USMTF) messages. JOTS allowed the Fleet Command Centers to interface with command ships and other shore installations. Through the use of a tactical database manager (TDBM), JOTS provided a consistent tactical battlespace picture for all supporting warfare commanders afloat and ashore. [Ref. 17:p. 60]

The original prototyping effort of JOTS led to the development of the JOTS Command and Control System by the late 1980s. The primary goal of JOTS was to integrate information systems onto common hardware and software platforms to allow the sharing of databases as well as maximize limited shipboard space. JOTS-derived systems have since been installed onboard over 200 Navy ships, at several US Navy shore intelligence centers, onboard US Coast Guard vessels and allied ships, and at various allied shore facilities. As JOTS matured further and as other C3I systems were developed and deployed, it became apparent that there was much duplication of software and functionality across systems. This duplication led to increased development, maintenance, and training costs and the goal of interoperability across systems was virtually non-existent. This low degree of interoperability led to conflicting information from multiple sources being provide to the operators and afloat decision makers. [Ref. 23:p. 1-1]

2. Navy Tactical Command System - Afloat (NTCS-A)

The Navy Tactical Command System - Afloat (NTCS-A) evolved from JOTS in the early 1990s from the consolidation of a number of prototypes of individual "stovepipe" shipboard command and control software programs, including the Flag Data Display System (FDDS), the Joint Operations Tactical System (JOTS), the Electronic Warfare Coordination Module (EWCM), and the Afloat Correlation System (ACS) [Ref. 15:p. 52]. Additional NTCS-A functionality was incorporated from other stand-alone or prototype

C4I systems such as the Prototype Ocean Surveillance Terminal (POST) and the Naval Intelligence Processing System (NIPS). Central to this consolidation effort was the abstraction of the afloat software into a common "core" set of software that could be used throughout the afloat community as the basis for their systems. This led to a set of common software originally called GOTS version 1.1.

The common core software concept was extended to the shore community to reduce development costs and ensure interoperability. This effort resulted in a collection of software commonly referred to as the Unified Build (UB) version 2.0 or GOTS 2.0. This software is now deployed both afloat, in NTCS-A, and ashore, in Operations Support System (OSS) known also as Navy Command and Control System-Ashore (NCCS-A). The strength of these two systems is that they are built on top of a common set of functions so that advancements and improvements in one area are immediately translatable to advancements in the other area. [Ref. 23:p. 1-1]

3. Operations Support System (OSS)

The Operations Support System (OSS) evolved from the functionalities of the Navy World-Wide Military Command and Control System (WWMCCS) Standard Software, Operations Support Group Prototype, Fleet Command Center Battle Management Program, and JOTS. This system is considered the shore installation variant of NTCS-A and is often referred to as Navy Command and Control System-Ashore (NCCS-A). By migrating the OSS into the JMCIS architecture, the Navy is seeking management economies of scale and performance enhancements in OSS.

4. Joint Maritime Command Information System (JMCIS)

The Joint Maritime Command Information System (JMCIS) represents the next logical step in the evolution of Navy C4I systems. The addition of functions to NTCS-A has led to the creation of a new version of that system, which has been designated JMCIS. JMCIS is described as a "overarching architecture" that is still evolving as fleet operators refine C4I requirements and the functionality of other systems is migrated to the JMCIS architecture. The JMCIS approach to adding new functionality instead of building new systems allows the Navy to benefit from a single-configuration management approach. The system software provides the basic functions, such as display control, message-traffic control, and specific applications for various ship classes. [Ref. 15:p. 56]

Programmatically, JMCIS has consolidated the functions of NTCS-A and its complimentary ashore program, the OSS. The two systems are expected to form a significant core of the ongoing development of service-wide C4I architectures, referred to as the Global Command and Control System (GCCS), that will continue to consolidate the C4I initiatives of the individual services. [Ref. 15:p. 56]

5. Global Command and Control System (GCCS)

GCCS is a Joint Staff sponsored program envisioned by the C4I for the Warrior concept and represents the next step in the evolution of command and control systems. When fully implemented, GCCS will embody a network of systems providing the Warrior with a full complement of command and control capabilities. As part of the C4I for the Warrior concept, GCCS is evolving into a global, seamless "Infosphere" capable of meeting the Warrior's fused information requirements. [Ref. 18:p. 25]

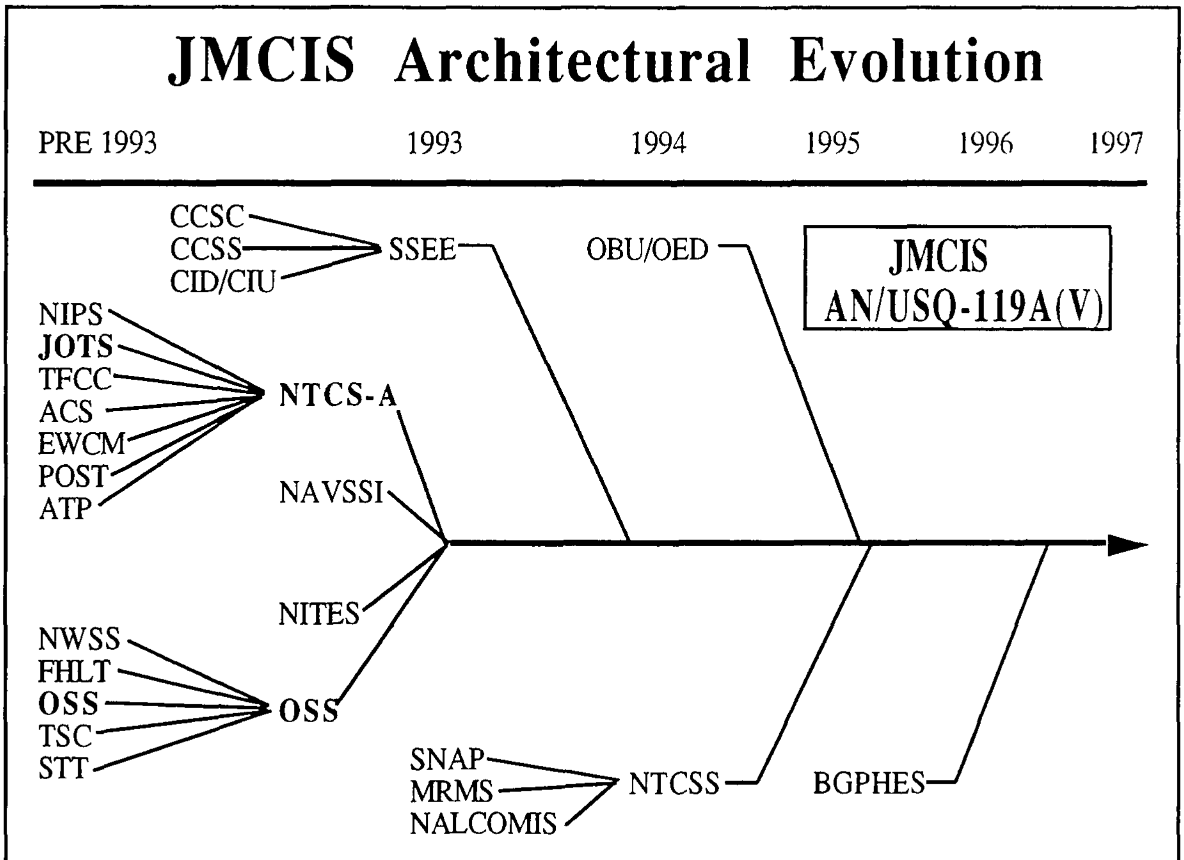

Figure 11: Systems Migration [Ref. 24]

6. Systems Migration

The proceeding description of the Navy C4I systems evolution focused primarily on the core systems only. In addition to the primary systems described, several other systems have merged functionality into these core C4I systems as the evolution progressed. Figure 11 shows the various systems that have "migrated" toward the core environment that is currently the JMCIS architecture. Note the pre-1993 systems that represent a myriad of functionality that integrated into follow-on systems. The current status of the evolution is JMCIS. However, this evolution will continue, adding the additional functionality of both traditional C4I systems as well as administrative support systems such as the

Shipboard Non-Tactical ADP System (SNAP). Table 5 provides a listing of full names for the systems that have been or are scheduled to be migrated to the JMCIS architecture.

TABLE 5: MIGRATION SYSTEMS

Acronym	Full System Name
ACS	Afloat Correlation System
ATP	Advanced Tracking Prototype
BGPHES	Battle Group Passive Horizon Extension System
CCSC	Cryptologic Combat Support Console
CCSS	Cryptologic Combat Support System
CID/CIU	Cryptologic Interface Device/Unit
EWCM	Electronic Warfare Coordination
FHLT	Force High Level System
JOTS	Joint Operational Tactical System
MRMS	Maintenance Resource Management System
NALCOMIS	Navy Aviation Logistics Command Management Information System
NAVSSI	Navigation Sensor System Interface
NIPS	Naval Intelligence Processing System
NITES	NTCS-A Integrated Tactical Environmental Subsystem
NTCS-A	Navy Tactical Command System - Afloat
NTCSS	Navy Tactical Command Support System
NWSS	Navy WWMCCS Software Standardization
OBU/OED	Ocean Surveillance Information System (OSIS) Baseline Upgrade
OSS	Operations Support System
POST	Prototype Ocean Surveillance Terminal
SNAP	Shipboard Non-Tactical ADP Program
SSEE	Ships Signal Exploitation
STT	Shore Targeting System
TFCC	Tactical Flag Command Center
TSC	Tactical Support Center

C. THE JOINT MARITIME COMMAND INFORMATION SYSTEM (JMCIS) ARCHITECTURE

1. Description

The Joint Maritime Command Information System (JMCIS) is built as an architectural framework to meet specific Navy and DoD command and control (C2) capabilities. Similar to the Microsoft Windows environment, JMCIS provides an environment for applications to consolidate common functions. In Microsoft Windows, multiple applications share common utilities such as printing and file management, rather than duplicating those functions for each application. For C2 systems, JMCIS provides various common utilities such as mapping and tactical database display functions among others. This collection of utilities comprises the JMCIS core which is maintained and expanded based upon the migration of legacy systems and improvements to existing JMCIS applications.

JMCIS is designed to be an open system that enables true functional integration through standard display, data, and communications management. JMCIS offers an "integration of systems" versus "federation of systems." That is, it is not sufficient for two applications to execute on the same hardware and be simultaneously available to an operator. In addition to sharing common utilities, the applications must also share data. This approach represents a key difference between the JMCIS approach and the Microsoft Windows environment. [Ref. 23:p. 1-11]

The consolidation of functions into a Common Operating Environment (COE) allows all applications to access the most efficient utility and provides the opportunity to easily update the core utilities with improved versions. In traditional client/server style, JMCIS servers provide core services to the rest of the network and each workstation may have either the same or different application software running. Figure 12 shows the JMCIS software architecture. Various applications can be selected to run "on top" of the COE. Those applications may have originally served as the base functionality for a previous Navy, Marine Corps, or other service's stand-alone application. [Ref. 23:pp. 1-3]

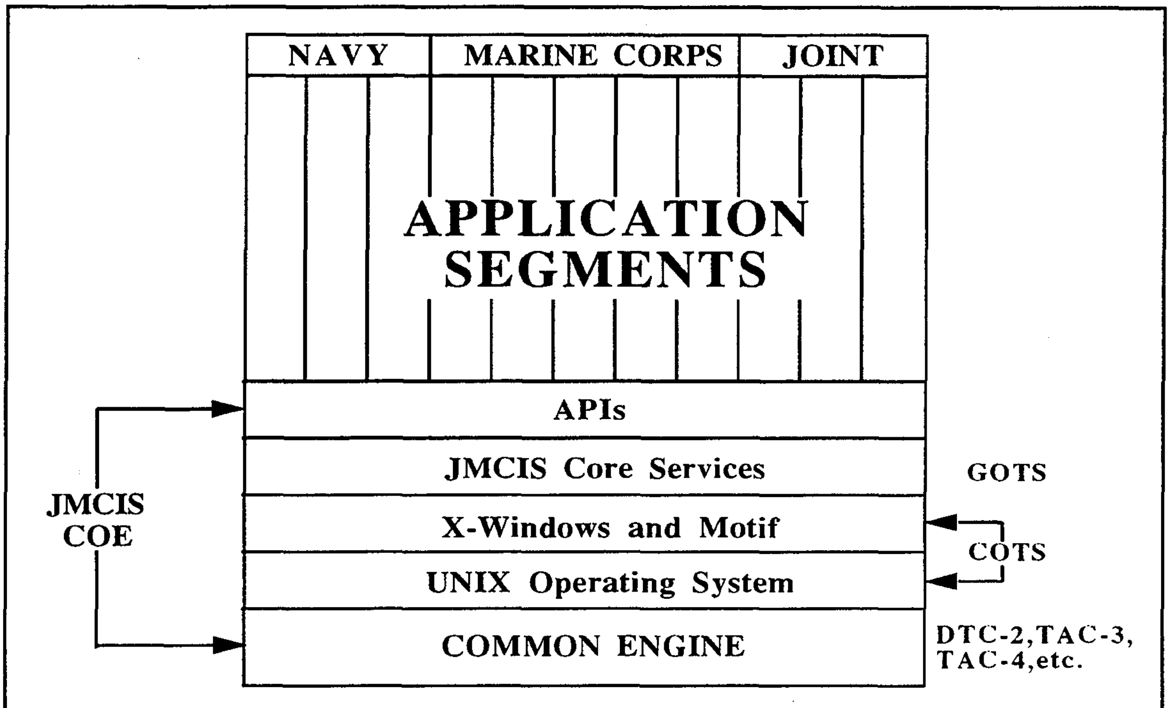

Figure 12: JMCIS Software Architecture [Ref. 24]

JMCIS is an umbrella system that has incorporated various functionalities and attributes of previous command and control systems. The philosophy of incorporating other systems capabilities and functionality is not unique to JMCIS; rather, it is a trait inherited from previous systems. The Joint Operational Tactical System (JOTS), Navy Tactical Command System - Afloat (NTCS-A), and Operations Support System (OSS) are examples of systems that applied this same evolutionary methodology and directly influenced the development of JMCIS. The core software GOTS 1.1 was compiled for use throughout the afloat community as the basis for all C4I systems. GOTS 2.0 was called the Unified Build (UB) 2.0 and was developed to include the ashore community in order to further increase system interoperability. The system was also designed to operate on the Tactical Advanced Computing (TAC) family of computers, as a non-proprietary, open architecture that could be easily transported to subsequent improved versions of the TAC. [Ref. 23:pp. 1-3]

2. System Software Components

The heart of JMCIS is the collection of software components. JMCIS should be viewed as a collection of several related items required for developing an information system. JMCIS provides a clearly defined set of functions or modules which constitute a C4I system. These functions and the software which implements them form the JMCIS core services and include track management, correlation, communications, and tactical display components. Additionally, JMCIS provides a precisely defined architecture for how the modules will interact and fit together.

a. Common Operating Environment (COE)

The JMCIS Common Operating Environment (COE) consists of the UNIX Operating System (OS), X-Windows graphical windowing system, and Motif standard styles. In addition to the COTS software, the JMCIS COE provides core software for receiving and processing messages, correlation, updating the track database, and software for generating displays. The JMCIS COE provides for unattended message reception, processing, and track management so that an operator need not actually be logged in to a workstation. [Ref. 23:p. 2-1]

b. Unified Build (UB)

The Unified Build (UB) is the foundation for all JMCIS software. The UB is a set of software components that include the Common Operating Environment (COE) and a standard software base for central applications and library functions necessary for basic command, control, and supporting functions. The UB is not a deliverable system by itself, but is delivered to developers for use in building an end system.

c. JMCIS Segments

A segment is a software application that operates in the JMCIS environment utilizing core functionalities for common operations. Segments access the core functionality through a standard set of Application Program Interfaces (APIs). The standard set of APIs is managed by the core developers and is the access vehicle to core functionality. Unique functionality for individual segments is provided by the individual applications' source executable code. JMCIS segments provide a collection of already developed and tested Tactical Decision Aids (TDAs) and support functions (range and bearing calculations, CPA, etc.) that may be incorporated into a particular JMCIS variant.

There are different types of JMCIS segments depending on the level of integration and the functionality required by the segment. Most JMCIS developers will be creating software segments that represent options to add to the JMCIS core functionality. As previously described, software segments access the JMCIS core services through APIs. Likewise, data segments allow data files to be treated just like any other JMCIS segment, each loaded individually. [Ref. 23:p. 3-7]

The functionality of many previous stand-alone systems have been integrated into current JMCIS segments. Figure 13 depicts many of the JMCIS segments that have been created. Some segments have retained the name of the original system from which the functionality evolved, such as JOTS. Other segments consist of various functionality required for specific missions or analytical techniques not available within the Unified Build software. New functionality is added to the base JMCIS functionality by creation of a new JMCIS segment.

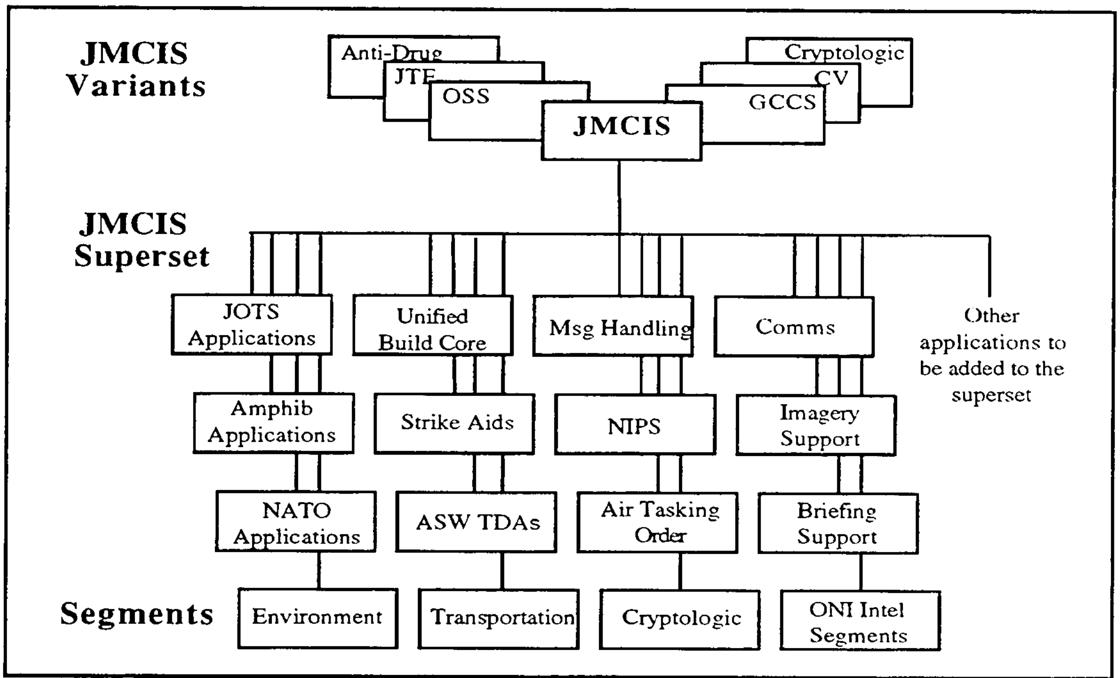

Figure 13: JMCIS Superset Structure [Ref. 25]

d. JMCIS Variant

A variant is a subset collection of segments, from the JMCIS Superset, installed for a specific mission area such as mission planning or battle group database management. Figure 13 also shows example variants, such as a Joint Task Force (JTF) or the aircraft carrier (CV) variant. The boxes labeled as JMCIS segments are plug-in customization modules which define the JMCIS variant and control what access an operator has to services provided by the core. These are in effect what actually define the system and distinguish one JMCIS variant from another. The collection of various JMCIS segments are simply customized modules that define the JMCIS variant. [Ref. 23:p. 2-8]

3. System Hardware Components

The JMCIS software described above is currently supported by two hardware platforms, the DTC-II SUN-based systems and the TAC-3 Hewlitt-Packard-based systems in a client/server configuration. Although these are presently the only two platforms supported for testing and configuration management purposes, the JMCIS software has been successfully ported to other vendor-hardware platforms including the use of PCs with appropriate COTS software configurations such as X-terminals. The JMCIS software, as delivered, is capable of supporting the standard components shown below:

TABLE 6: STANDARD JMCIS HARDWARE CONFIGURATIONS

[Ref. 23:p. 2-13]

TAC-3 Standard Components	DTC-II Standard Components
HP-730 CPU	4/300 or 4/110 SUN CPU
32 MB RAM	32 MB RAM
1.2 Gigabyte Disk Drive	500 MB Hard Disk
G1 Graphics Card	CG6 Graphics Card
19" Color Monitor	19" Color Monitor
Trackball/Mouse	Trackball/Mouse
Keyboard	Keyboard
Tape Drive	Tape Drive

4. Objectives of the JMCIS Architecture

While examining the evolution of the JMCIS concept and system architecture, there are a number of objectives which become apparent. The objectives include technical considerations such as software reusability, enforcement of common "look and feel", and standardization of interfaces. These technical objectives provide the potential for significant cost savings and further development acceleration. The objectives include:

- Commonality - Developing a common core of software that will form the foundation for Navy and Joint systems.

- Reusability - Developing a common core of software that is highly reusable to leverage the investment already made in software development.

- Standardization - Reducing program development costs through the commonality and reusability objectives and through adherence to industry standards. This includes the use of commercially available software components whenever possible.

- Engineering Base - Through standardization and an open JMCIS architecture, establishing a large base of trained software and systems engineers.

- Training - Reducing operator training costs through enforcement of a uniform, human-machine interface, commonality of training documentation, and a consistent "look and feel."

- Interoperability - Solving the interoperability problem (at least partially) through common software and consistent system operation.

- Certification - Providing a base of certified software so that systems performing identical functions will give identical answers.

- Testing - Increasing the amount of common, reusable software to reduce testing costs since common software can be tested and validated once and then applied to many programs.

[Ref. 23:p. 1-13]

D. ONI ARCHITECTURE DEVELOPMENT

As the US Navy's lead C4I systems development agency, the Naval Command, Control, and Ocean Surveillance Center (NCCOSC), Research, Development, Test, and Evaluation Division (NRaD) has developed a Program Management Plan (PMP) for transitioning ONI systems to the JMCIS architecture. The architectural approach is intended to enhance analyst productivity and systems functionality while maintaining future IS expenditures within fiscal boundaries. This approach will support ONI's vision of providing maritime intelligence to consumers and afford the greatest degree of compatibility with C4I systems converging under the JMCIS and GCCS architectures. JMCIS software currently provides the core command and control (C2) system capabilities for GCCS. JMCIS also provides the overall C4I architecture for the Ocean Surveillance Information System (OSIS) Evolutionary Development (OED) effort which will provide an integrated intelligence analysis capability at the Joint Intelligence Centers (JIC). [Ref. 26:p. 1]

The NRaD plan calls for transitioning ONI legacy systems to standardized hardware and software, and developing any new functionality within the JMCIS architecture. The heart of this effort is the integration of ONI systems functionality into new Intelligence Segments within the JMCIS architecture. Additionally, the plan calls for the consolidation of existing maritime databases into a centralized system. This section will describe the target JMCIS architecture that will incorporate ONI intelligence systems and databases.

1. JMCIS Intelligence Segments

The target architecture envisioned by NRaD for ONI systems includes integration of current systems functionality into JMCIS Intelligence Segments and will, therefore, consist primarily of new intelligence segment development. The functionality of the following ONI intelligence systems and applications, previously described in the baseline characterization, will be incorporated into the JMCIS segments:

- Automated Merchant Identification Ship System (AMIDSHIPS)
- Collection Requirements Management Application (CRMA)
- Joint Maritime Information Element (JMIE)
- Merchant Watch (MerWatch)
- SeaView
- SeaWatch III

Additionally, the functionality of two systems that are managed by ONI that currently support other intelligence sites will be added to the following JMCIS Intelligence Segments:

- Ocean Surveillance Information System (OSIS) Baseline Upgrade / OBU Evolutionary Development (OBU/OED)
- Joint Deployable Intelligence Support System (JDISS)

The functions of the JMCIS Intelligence Segments will include analytical tools that currently exist within the SeaWatch III system, the SeaView system's data manipulation and presentation functions, and civil maritime analysis functions derived from the requirements of the MerWatch system not already available in other JMCIS segments. The additional functionality from SeaWatch III, SeaView, and MerWatch will complement current JMCIS 2.1 intelligence segments that include the functionality of CRMA and

JDISS. The OED system functions operating in the multi-level secure (MLS) environment will also constitute a future JMCIS segment. [PMP] The initial baseline for the JMCIS intelligence segments will be the JMCIS 2.1 software which includes the COE. The baseline will consist of the Unified Build (UB) segment and the other JMCIS 2.1 optional segments. [Ref. 26:pp. 2-3]

The JMCIS configuration for ONI intelligence analysis will consist of the following software segments with functionality summarized:

a. Unified Build (UB) Segment

Chart-2 Mapping	Executive Menu Service
Track Database Manager	External Communications
Alert Services	Applications Toolkit
User Interface Toolkit	Printer Utilities

b. Civil Maritime Analysis Segment (CMAS)

MerWatch Release C.1 Functions	Maritime Transportation Model
JMIE Functions	Link Analysis
SeaWatch III Functions	Access to Maritime Databases
Organization Module and DB Process	Slide Preparation
Spread Sheet	Graphic Drawing
Report Generation	Maritime Data Alerts
Optical Character Reader	

c. Data Visualization Tools (DVT) Segment

Data Listing	Iconify-by
Color-by	Count-by
Histogram	Scattergram
Operations Clock	Get Data (Database Retrieval)
Format Specification	

d. JMCIS Expedited Text Search (JETS) Segment

Document Search	B1 Level Security Tags
Narrative/Formatted Message Search	Word Processing Tools
Pre-Loaded High Use Documents	CD-ROM Interface

e. Database Browser Segment

Generic RDBMS Database Scan

f. Additional Intelligence Segments

JMCIS segments for the CRMA and JDISS systems are being developed separately. The functionality of these segments will be available to ONI intelligence analysts as optional segments that can be loaded with the baseline JMCIS intelligence segments. [Ref. 26:pp. 4-7]

2. Database Segment Development

As previously discussed, the NRaD plan calls for the consolidation of existing ONI maritime databases into a centralized system. This database conversion effort will constitute the development of the National Maritime Intelligence Database (NMID) within the JMCIS architecture. The NMID will then be accessible by JMCIS segments including the newly created Intelligence Segments for ONI analyst use. The current JMCIS Central

Data Base Server (CDBS) for afloat systems shall incorporate the NMID database design and structure as appropriate. ONI baseline system databases to be consolidated into the NMID include:

- SeaWatch III Database
- Merchant Ship Characteristics (MSC) Database
- Naval Intelligence Database (NID)
- Joint Maritime Information Element (JMIE) Database
- AMIDSHIPS Imagery Database.

[Ref. 26:p. 7]

3. Technology View

The JMCIS development and integration process supports both the SUN DTC-2 and Hewlitt-Packard (HP) TAC-3 family of computers and peripherals in a client/server configuration. Figure 14 shows a generic view of the JMCIS network configuration using the TAC-3 and DTC-2 platforms with access available to PCs. The NRaD plan calls for the re-use of existing ONI hardware in the target architecture. The overall design calls for a distributed architecture of server systems permitting the addition of other servers and transparent distribution of database tables. Existing JMCIS database management (Relational Data Base Management System - RDBMS) software permits the automated routing of database queries across a network and the construction of a composite retrieval report. [Ref. 27]

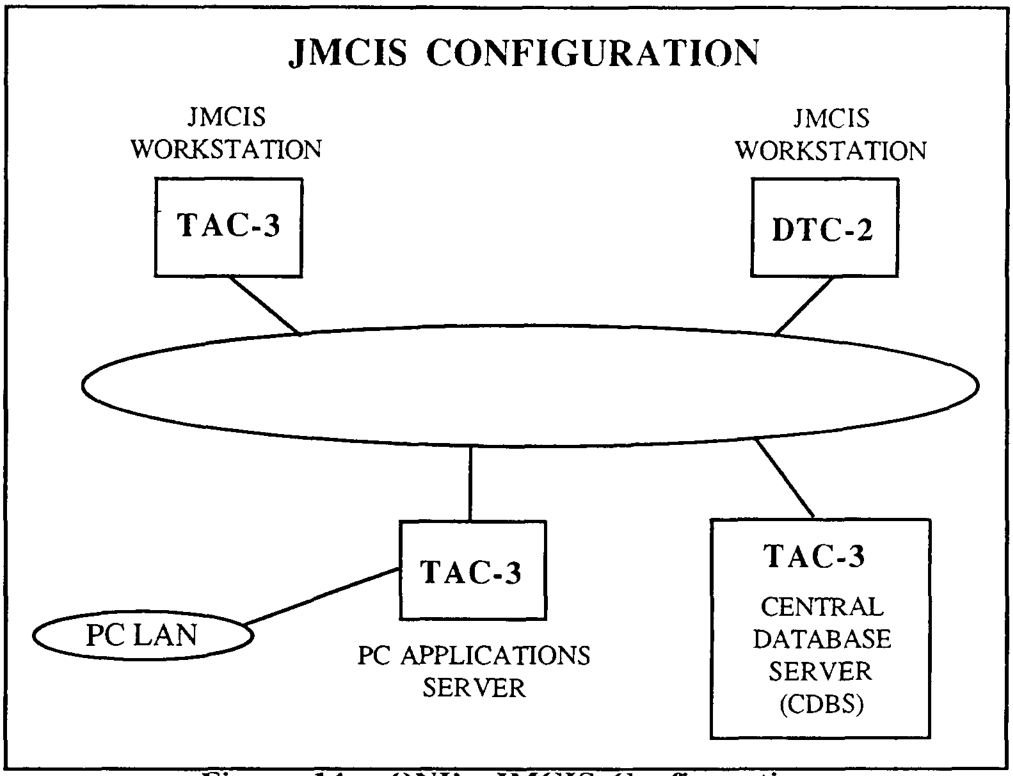

Figure 14: ONI's JMCIS Configuration

a. Re-use of PCs as X-Windows Database Clients

Currently, ONI intelligence analysts use 386/486 PCs as data entry terminals for inputing NID data into the VAX Oracle database. With the conversion of the VAX to a UNIX database system, continued use of PCs would be cost-effective and provide access to Windows and DOS tools and applications such as spreadsheets and word processors. The technical approach recommended is to obtain a high enough performance COTS package to allow the PCs to operate as X-terminals which access the UNIX database system. This would allow full database edit and browse functions to be made available to all PC analysts. [Ref. 27]

b. Re-use of SUN 4/690 Servers

GOTS high speed text search software and indexed reference and analysts documents would be hosted on these servers. These systems are oriented to server functions and with large capacity disks would be a cost effective storage and search system. [Ref. 27]

c. Re-use of ONI SUN Sparc 2/10 Workstations

These client workstations would be able to perform all data base queries to the SeaWatch III server, display, and manipulate JMCIS maps and tracks, and perform high speed text search retrievals from SUN and HP servers. [Ref. 27]

VI. OPPORTUNITY IDENTIFICATION

A. INTRODUCTION

The TAFIM SBA Planning Guide describes opportunity identification as the phase "... where projects necessary to move the organization from its current environment to its target environment are identified." This phase defines the "opportunity vision" for the organization. Specific categories for evaluating implementation "payoff" opportunities are offered by the SBA Planning guide. These categories are the specific objectives for the DoD TAFIM and include:

- Improving user productivity
- Improving development efficiency
- Improving portability and scalability
- Improving interoperability
- Improving vendor independence
- Reducing life-cycle costs

The key deliverable of this phase is a high-level understanding of the opportunities at hand. The "... entire objective is to describe the nature of the target architecture opportunities and the role they will play in closing the gap between the baseline environment and the target architecture." [Ref. 7:Vol. 4,p. 5-5,6]

B. DESCRIPTION OF PROJECT OPPORTUNITIES

1. User Productivity

To the end user, JMCIS represents a information system which is distributed across a network of workstations. System operators are able to access all required functionality from any workstation, regardless of the individual workstations physical location or the actual location where the processing is taking place. The user is presented with only the functionality needed to meet their mission with other unneeded functionality hidden to prevent overwhelming the user. An operator with a different set of tasks is presented with a different set of functionality, but both operators perceive that the system looks and operates in the same way. JMCIS will appear to the operators as the identical information system in use by other military commands and intelligence centers with completely different mission objectives. This commonality is of increasing importance with the expanded role of the services in joint operations. [Ref. 23:p. 1-7]

Operator training is simplified by conformance to identical standards. Training issues are significant because an operator may be expected to have to use multiple systems which behave completely differently, are equally complex with their own subtleties, and which give slightly different answers. Operator turnover is rapidly reaching the point where the time it takes to train an operator is a significant portion of the time the operator is assigned to his current tour of duty. With the JMCIS system being deployed and delivered to both the afloat and ashore user communities, a commonality between sites will greatly reduce the training required. Through the use of an open architecture and standardization of user interfaces, both operator and maintenance personnel familiarization with a single system will translate directly to other systems using similar hardware and software environments.

2. Development Efficiency

From the perspective of a system program manager, JMCIS presents the opportunity for a program that encompasses several programs. With the impact of decreasing DoD budgets, program managers can maintain program viability and achieve considerable savings by constructing their system within the JMCIS architecture. Within the current budget constraints, these potential savings appear as the only feasible option for many programs. [Ref. 23:p.1-7]

The greatest opportunity afforded by JMCIS for program managers may be the reuse of existing and proven software. Rather than concentrating scarce development resources on recreating building blocks, the resources can be more appropriately applied to customization and development of functionality that is not currently available, allowing the focus of attention on mission uniqueness.

From the perspective of a system developer, JMCIS is an open architecture and a software development environment that offers a collection of services and already built modules. The system developer's task is to assemble and customize the existing components from JMCIS while developing only those capabilities unique to a particular mission requirement. In many cases, this will amount to adding new "pull-down" menu entries. The JMCIS developers provide detailed instructions on how to make applications or systems compliant with the JMCIS architecture. These instructions include details on the standard user interface and the procedures for using core functionality via APIs. The core functionality has been previously developed and tested, and the developer need only produce segments that are unique in functionality to their particular application or mission area. The JMCIS COE establishes standards and provides baseline functionality so that the system developer's task is to extend this baseline and add supplemental functionality to meet mission specific requirements. [Ref. 23:p. 1-7]

3. Portability and Scalability

When delivered to operational sites, the JMCIS software is installed on workstations that may be grouped together by mission area into physical spaces or other logical arrangements. Within a space, software will be installed on one or more workstations, depending on the JMCIS variant. The same software tapes can be used to load any workstation regardless of the site or location of the workstation in the space. During the installation process, only that portion of the JMCIS Superset required for a particular workstation is actually loaded onto the workstation. From a general configuration management perspective, only one set of tapes are required to be controlled. The same set of software tapes can be use throughout the site. From an installation perspective, the site installer doesn't need to worry about different tapes to load on different workstations depending upon function. Functionality of each workstation can be tailored to that workstation. From a system design perspective, the ability to create JMCIS variants allows the flexibility of loading and executing only that software which is required to support a mission requirement. [Ref. 23:p. 1-22]

Designed to be hardware independent, the JMCIS the software successfully operates on a variety of Silicon Graphics, HP, Sun, DEC, and PC platforms. It can generally run on any hardware system which supports UNIX System V, X-Windows, and Motif. While JMCIS has been installed on a variety of platforms with a wide range of platforms used in its development, it is thoroughly tested only for DTC-II and TAC-3 configurations and is thus formally supported only for these two computer platforms. [Ref. 23:p. 7-4]

JMCIS is designed as a client/server architecture so that core processes may be distributed across a LAN or run on a single workstation. Thus, JMCIS is scaleable from a single workstation up to a network of workstations. The largest JMCIS installation to date is approximately 35 workstations supporting approximately 50 simultaneous operators. Some workstations have multiple keyboards and monitors to support more than one user. [Ref. 23:p. 7-3]

4. Interoperability

The principle advantage of the JMCIS architecture is that participating communities and organizations will be interoperable because they use exactly the same software base. With the JMCIS approach, not only is the same software used by participating communities as building blocks, but the same system (JMCIS) is deployed to participating communities. The JMCIS philosophy realizes that interoperability problems are usually caused by differing or incorrect interpretations of standards. For this reason, the JMCIS architecture calls for the use of identical software to perform common functions. The primary goal of JMCIS is to have a body of C4I software that can be configured to support a variety of requirements while assuring interoperability among sites. The JMCIS architecture is being deployed throughout the joint command and tactical communities and will serve as the basis for future command and control systems migrating to the Global Command and Control System (GCCS).

As expressed in the Joint Staff's *C4I for the Warrior*, the ability to pull information from any location at any time gives the Warrior both more flexibility and the skill to tailor information to his specific needs. JMCIS offers the Warrior the ability to pull information from external sources. The Track Database Management (TDBM) system is possibly the most important piece of the JMCIS system. The TDBM, coupled with the extensive communications capabilities of JMCIS, allows greater interoperability with external sources and databases. The TDBM provides standard procedures and formats to add, delete, modify, and merge basic track data among the various workstations on the local area networks. [Ref. 23:p. 2-22]

5. Vendor Independence

One of the objectives of JMCIS is to avoid having command and control systems tied to a specific hardware platform or proprietary system. The system is designed to be easily transported from one version of TAC computer to the next with the capability of exploiting the improved capability of the now upgraded system. TAC hardware, COTS and GOTS software, and both government and industry standards, are to be used for all current and future JMCIS development. With the open architecture and commercial standards used by JMCIS, advances in computing platforms can be easily incorporated by simply changing the system's host machine.

The JMCIS software is also not vendor proprietary except for the COTS products such as UNIX, X-Windows, and Motif, which are required for the JMCIS environment. These COTS products are proprietary implementations of industry standards. All other software has been developed under contract to the US Navy. The government retains distribution rights for the government-funded software and data. [Ref. 23:p. 7-3]

The financial savings of moving toward an open architecture environment are also significant. While hardware costs have experienced a steady downward trend over the last several years, costs for proprietary software have greatly increased. The use of COTS software products counters the problem of increasing costs by allowing the developer of a product to spread the cost of development among all users of the product. Achieving these economies of scale is the major cost saving characteristic of the JMCIS open architecture environment.

The commercial marketplace moves at a faster pace than the government or DoD marketplace and advancements are generally available at a faster rate. Figure 15 presents the dramatic increase in performance between successive TAC system procurements. Use of commercial products has the advantage of lowering cost by using already developed and produced items, increases the probability of product enhancements because the marketplace is larger, and increases the probability of standardization.

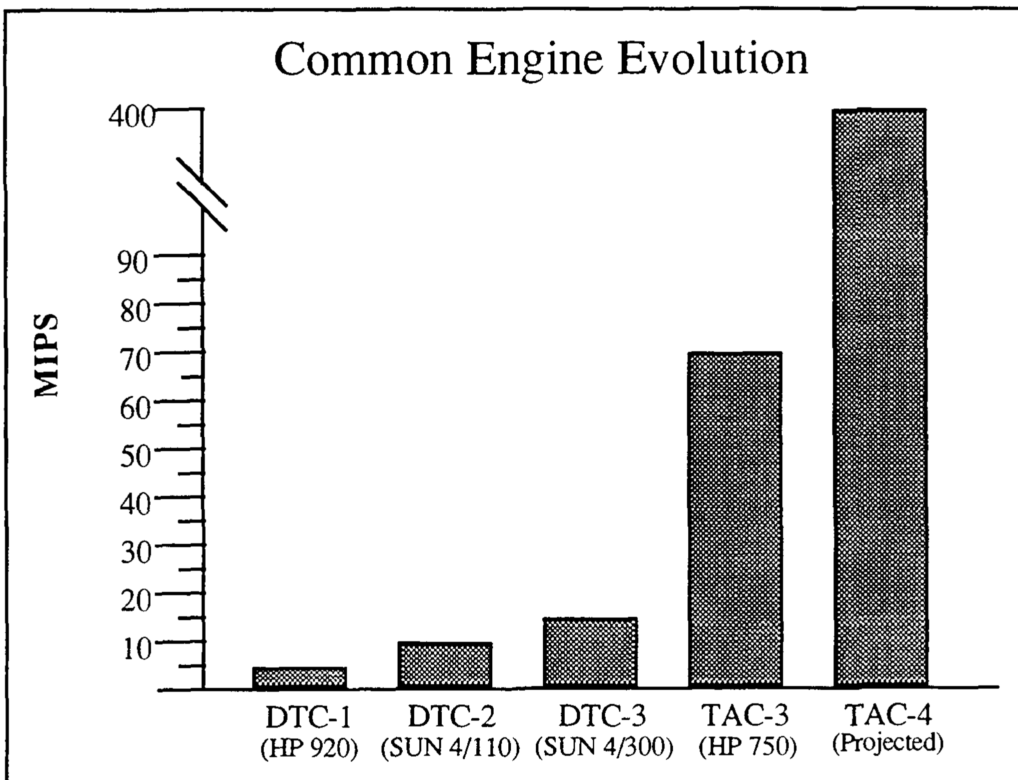

Figure 15: Platform Performance Improvements [Ref. 32]

Technological gains occur rapidly in the computer industry. The commercial computer industry introduces new systems and new capabilities approximately every 18 months. With the average DoD major automated information system acquisition taking over 24 months from requirements specification to system delivery, DoD is constantly delivered obsolete systems. However, open systems architectures can offer a solution to this technological dilemma. The basis of open systems are the common development standards from which products can be developed using nonproprietary specifications. The advantages of using an open systems architecture to an organization the size of DoD present the most efficient and practical approach to the use of hardware and software.

6. Life-Cycle Costs

With JMCIS, the system life-cycle cost is reduced by development and maintenance of a single system. The US Navy has traditionally funded development and redevelopment of the same functionality across systems. Redevelopment is frequently necessary because of technological changes as algorithms are improved or as hardware becomes faster. However, much of the development cost is due to a change in who the developer is as contracts expire, or lack of coordination between programs that share common requirements.

Significant savings can also be achieved by supporting a reduced number of lines of code. This reduction in lines of code is accomplished by implementing a common core of software and only producing the unique portions of the JMCIS segments. Initial analysis of candidate command and control systems eligible for migration to JMCIS has revealed significant reductions in post-deployment software support. A study conducted jointly in 1993 by NRaD and the Marine Corps Tactical Systems Support Activity (MCTSSA) revealed significant redundancy in software among Marine Corps command and control (C2) systems. The study found that when compared to a common core of software, such as that existing in the JMCIS/GCCS Common Core, these C2 system could achieve a reduction of 45 to 84 percent in software lines of code.

Figure 16 the shows potential reduction in source lines of code that could be achieved in an air defense system and an intelligence analysis system if they were converted to software segments on top of a common core of software. The MCTSSA study found that the vast majority, over 70 percent, of code in these systems was used for Computer Software Configuration Items (CSCI) such as mapping/overlays, track management, message processing, communications processing, security, and system administration. Each system studied had its own separate software to support these common functions. [Ref. 28]

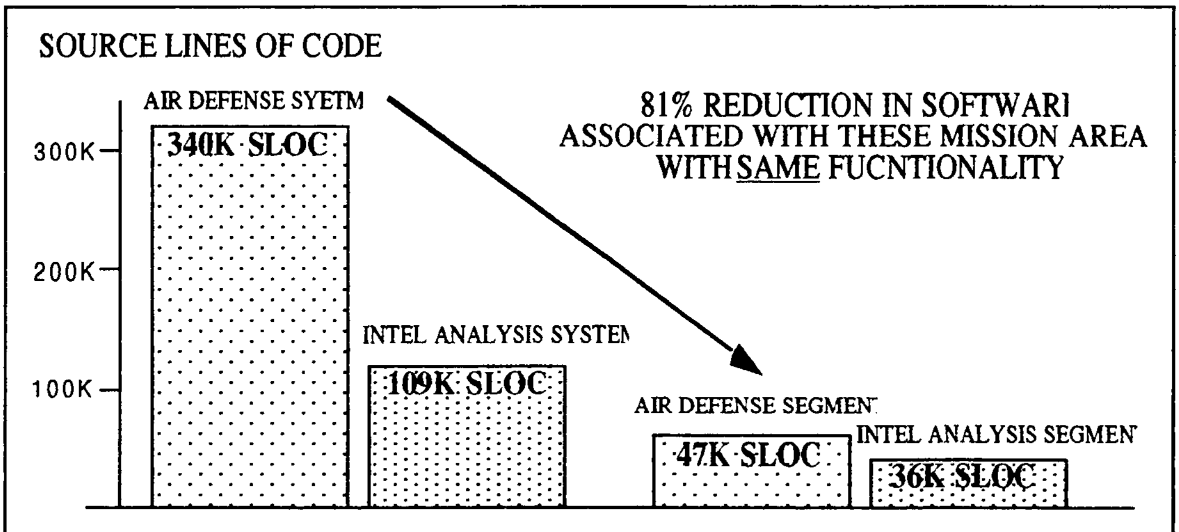

Figure 16: Example of Software Reduction Using a Common Core
[Ref. 28]

C. OPPORTUNITIES FOR ONI

The project opportunities presented in the previous section outline the potential benefits to DoD offered by the JMCIS architecture and its established development procedures. As outlined, the opportunities presented are directly aligned with the objectives of the DoD TAFIM. Likewise, the objectives of the JMCIS architecture conform with ONI's IT Principles as outlined in Chapter III. This section will specifically address the JMCIS project opportunities with regard the potential benefit to ONI addressing each IT Principle. In doing so, this analysis will attempt to further link the target architecture to the strategic vision of ONI.

1. Meta-Principles

a. Implement a demand-pull capability for ONI's intelligence dissemination.

Integration of ONI systems with the joint command and tactical communities is an essential step toward achieving the goal of a demand-pull dissemination capability. While migration toward the JMCIS architecture does not in itself provide the demand-pull capability, it provides the critical connectivity to the operational consumer required. Further development of ONI systems, products, and services will be required to fully achieve the objectives of this IT Principle. The JMCIS architecture provides the means to implement a demand-pull capability for ONI's intelligence dissemination.

b. All ONI systems development will remain consistent with DoD-wide strategic IS initiatives.

The JMCIS architecture and its development procedures are consistent with DoD-wide strategic IS initiatives. Migration to the JMCIS architecture and the participating defense community ensures that ONI systems will conform to the standards of the CIM initiative. Initiatives such as the *Copernicus* architecture emphasize the concept of demand-pull data services. JMCIS is an evaluation of Navy C4I systems toward the achievement of the Global Command and Control System (GCCS) described in the Joint Staff's *C4I for the Warrior* initiative. Migration of ONI system to the JMCIS architecture ensures ONI systems development will remain consistent with DoD-wide strategic IS initiatives.

c. All ONI systems development will be accomplished in strict adherence with the JMCIS architecture and its established systems development procedures.

Adherence with the JMCIS architecture and its established systems development procedures will enable ONI to provide maritime intelligence to a broad consumer base while affording the greatest degree of compatibility with Navy C4I systems converging under the JMCIS and GCCS architectures.

d. All ONI systems development will be in consonance with DODIIS and TAFIM guidelines.

DoD-wide of C4I systems have undergone analysis in a migration system selection process as directed by the Assistant Secretary of Defense (C3I). The migration systems will form the foundation for future C4I architectures and are in consonance with DODIIS and TAFIM standards. JMCIS has been identified as the primary migration system for Navy C2. Migration of systems to the JMCIS architecture ensures ONI systems development will remain consistent with DODIIS and TAFIM guidelines.

2. Information Management

a. Create the National Maritime Intelligence Database (NMID).

The consolidation of current ONI databases into the JMCIS architecture as a data segment will constitute the initial implementation of the NMID concept as envisioned in the ONI Strategic Plan. The NMID is intended to provide on-line query response services to the consumers. The JMCIS architecture provides the essential on-line connectivity required to a broad range of consumers. The integration with the user / customer has been identified as the key to success for the NMID.

3. Application Management

a. Systems architecture development must retain the unique analytical functionality that current applications provide to ONI intelligence analysts.

The JMCIS architecture calls for the integration of system functionality through the development of JMCIS software segments. Unique analytical functionality that does not exist in current JMCIS components must be integrated into a JMCIS software segment. The functionality of ONI systems are planned for integration into a range of JMCIS Intelligence Segments.

4. Technology Management

a. ONI systems will migrate to an open systems, client/server environment.

JMCIS is designed as a client/server architecture so that core processes may be distributed across a LAN or run on a single workstation. JMCIS also offers an open systems architecture for which products can be developed using nonproprietary specifications. Migration of ONI system to the JMCIS architecture is in line with progress toward migration of ONI systems to an open systems, client/server environment.

D. SUMMARY ASSESSMENT

This chapter has presented an analysis of the opportunities presented by the JMCIS architecture in terms potential benefits both to the defense community and the strategic goals of ONI. As outlined, the opportunities presented by the JMCIS architecture and development procedures are directly in-line with the objectives of the DoD TAFIM. The JMCIS architecture provides an effective opportunity to keep pace with technological advancements while implementing open systems architectures and ensuring standardization of software and hardware for C4I systems among the services. The JMCIS approach to systems development addresses many recurring problems relative to procurement and development of DoD systems. It presents many opportunities to achieve the IS objectives of the DoD TAFIM while conforming to the IT Principles of ONI.

A summary of ONI's IT Principles and the opportunities offered by the JMCIS architecture is presented in Table 7. In addition to the opportunities offered by the JMCIS architecture and its development procedures to the defense community as a whole, JMCIS provides the opportunity to achieve many of the strategic objectives of ONI. Table 7 identifies two areas where significant progress toward ONI's strategic vision can be accomplished through migration to the JMCIS architecture. JMCIS offers the essential connectivity with the consumer that is a critical first step toward achieving a demand-pull dissemination capability. This connectivity coupled with the further consolidation of ONI databases into a centralized data segment within the JMCIS structure will be a significant step toward achieving the goal of providing the intelligence consumer with an on-line query response capability as envisioned for the National Maritime Intelligence Database (NMID).

TABLE 7: OPPORTUNITIES OFFERED BY JMCIS ARCHITECTURE

ONI's IT PRINCIPLES	JMCIS OPPORTUNITY
Implement Demand-Pull Dissemination	Progress Toward
Remain Consistent with DoD Strategic Initiatives	YES
Adhere to JMCIS Architecture Development Procedures	YES
Remain Consistent with DODIIS and TAFIM Guidelines	YES
Create the NMID	Progress Toward
Retain Unique Analytical Functionality	?
Open Systems, Client/Server Environment	YES

The basic idea of DoD and Navy standardization on a common, open systems architecture certainly makes sense. The effective migration of ONI system to the JMCIS architecture, however, will be a significant challenge. Again referring to Table 7, the challenge in the process of transitioning ONI systems to the JMCIS architecture will be ensuring that the unique analytical functionality currently supporting ONI intelligence analysts will be retained in the newly created JMCIS Intelligence Segments. While ONI can leverage the benefits of the well established pool of software segments and core services offered by the JMCIS architecture, careful consideration should be given to the risk associated with potential loss of functionality in the transition to the JMCIS architecture.

VII. MIGRATION ANALYSIS

A. INTRODUCTION

This phase in the TAFIM SBA Planning process and the final phase presented by this thesis will address the migration effort required to move an organization to a new or target architecture. Because most migration plans deal with migrating a current system or group of systems to a new system or target environment, a framework is needed to allow decision makers and system developers to evaluate the migration path selected. The procurement of an extensive information system or a complex upgrade to an existing system, as proposed for ONI, is an expensive and often risky proposition. A bad decision now could be very costly in terms of both expenditures and jeopardized critical mission functions. As the TAFIM SBA Planning Guide suggests, "Many worthwhile projects have floundered because migration was not adequately scoped prior to adoption." [Ref. 7:Vol. 4,p. V-1] Therefore, a thorough understanding of the risk is required and an effective evaluation framework is needed.

ONI's JMCIS architecture development effort involves a complex sequence of functionality migration and capability upgrades toward the target architecture described in Chapter V. Central to this effort is the creation of JMCIS Intelligence Segments that will incorporate the functionality of current ONI systems and offer the opportunity to add functionality as required. The JMCIS Common Operating Environment (COE) documentation offers a high-level "concept of operations" for integrating new functionality into a JMCIS segment. The suggested perspective for development is to consider JMCIS as a baseline collection of software which must be customized and supplemented. The objective is to build on top of JMCIS, not to decompose JMCIS into constituent parts and then build on top of some other architecture or body of software. Given this perspective, JMCIS should first be examined to determine which components satisfy the requirements as is, which need customization, which need extending, and what functionality is totally missing in JMCIS. The JMCIS COE documentation specifically recommends creating a matrix of required functionality and to check off the items as, performed by JMCIS, requires modification, or new functionality. This represents the initial development work that must be performed. [Ref. 23:p. 1-24]

This chapter is intended to present decision makers and system developers with a method for evaluating a complex migration effort such as that proposed for ONI. The chapter begins by defining many of the terms required to properly discuss and further analyze a migration plan. With appropriate terminology as a backdrop, this chapter then specifically addresses some concerns regarding the ONI migration. Finally, this chapter offers a suggested framework to properly evaluate and select a migration path. The framework focuses on maximizing value with an emphasis on functionality when scoping the migration problem. Example functionality/capability matrices are presented. This framework could be used for further analysis of migration alternatives that may be presented to ONI as the transition to the JMCIS architecture progresses. The framework is presented to offer decision makers a structured approach to evaluating migrations options. Further cost/benefit analysis will be required to make the best use of this framework.

B. MIGRATION TERMINOLOGY

1. System Functionality

System functionality is determined by the set of functions that are automated in a current system or desired for automation in a target system. A description of system functionality can often be found in a System Requirements Specifications document, such as exists for ONI's MerWatch system. The system functionality can be displayed in a functionality/capability matrix.

FUNCTIONALITY / CAPABILITY MATRIX

FUNCTIONS

TECHNOLOGICAL CAPABILITIES

	F1	F2	F3	F4	F5	F6	F7	F8	F9
TC1	X			X			X		X
TC2		X			X			X	
TC3	X			X		X	X		
TC4			X		X				X
TC5							X		X

Figure 17: Functionality / Capability Matrix
[Ref. 29:p. 42]

2. Technological Capabilities

In order to provide automated support to the set of required system functions, a system must offer a set of capabilities referred to as technological capabilities, such as data retrieval and chart displays. For example, to automate the data manipulation and fusion functions for the MerWatch system, data retrieval capabilities such as query interface, execution, and results are just a few of the technological capabilities required. The technological capabilities will also be displayed in a functionality/capability matrix. Figure 17 shows an example functionality/capability matrix used for comparison purposes so that the relationship between them can be clearly seen. For example, referring to Figure 17, in order to automate function F1, technological capabilities TC1 and TC3 are required. [Ref. 29:pp. 41-42]

3. Current or Base System

A current or base system is one that is currently in use or one that could be bought in the near term. It usually automates at least some key business functions. The current system's functionality is typically the basis for determining the functions and capabilities of the target system. The MerWatch system would be considered a base system as it currently exists.

4. Target System

A target system is one that will provide the desired level of automated support with the desired functionality at some future time. The target system's capabilities are the technological capabilities required to provide the automated support. The JMCIS system with the desired target functionality of the planned Intelligence Segments is considered a target system.

5. Migration Path

A migration path is an incremental series of upgrades to a base system that eventually leads to a fully functional target system. A viable migration path is one that is reasonable in terms of cost and risk and is acceptable to the operational and technical experts as well as program management. Figure 18 illustrates how a base system could take a different path toward achieving the required target system's capabilities. [Ref. 29:p. 43]

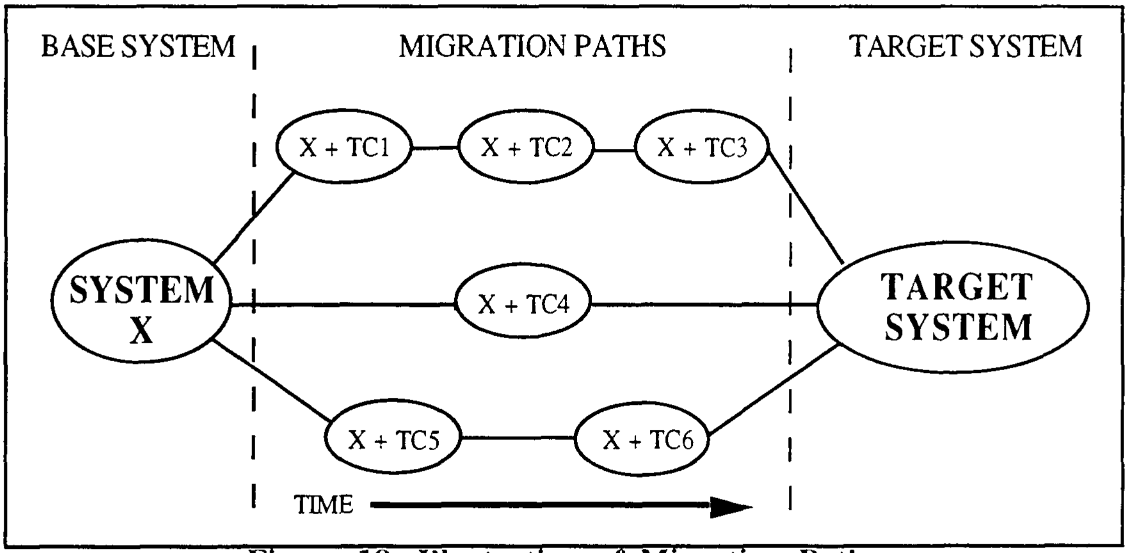

Figure 18: Illustration of Migration Paths

6. Migratory System

A migratory system is a future upgraded version of a particular base system and usually consists of the base system plus some additional technological capabilities. Several different migratory systems could be derived from a particular base system given different migration paths. The JMCIS system with less than the desired target functionality of the planned Intelligence Segments could be considered a migratory system for ONI at any time in the migration process prior to reaching the required target system capability. [Ref. 29:p. 43]

7. Value

The term value will be used in the discussion of the migration framework to characterize the benefit gained when a particular function is provided the required level of automated support. The added value or benefit to the intelligence analysis process because of the automation of a function could be measured in terms of a relative importance or weight. In either case, a value or benefit to the analysis as a whole can be associated with a target system's function. Values are discounted to their equivalent present values using a discount rate. Discounting converts future values to their equivalent present values. The framework will use the prescribed DoD discount rate of ten percent throughout the analysis. [Ref. 29:p. 44]

The term expected value will be used in the discussion when comparing decision alternatives. In many decision-making situations it is possible to obtain probability estimates for the possible outcomes, referred to as states of nature. The framework will consider various scenarios that have different outcomes. The expected value approach to decision-making evaluates each decision alternative in terms of its expected value. The expected value of a scenario is the value of its outcome adjusted for the probability of the scenario occurring.

8. Cost

The term cost will be used in the discussion of the migration framework to characterize the cost of adding technological capabilities to the base system along a migration path toward the target system. The framework will focus on the cost associated with a particular technological capability and its integration into an migratory system. Costs could include both initial conversion costs and life-cycle operating costs.

The cost of adding technological capabilities in different time periods can be aggregated by discounting the costs to a common point in time. All costs can then be expressed in terms of the present using a discount factor. Discounting converts future costs into their equivalent present costs using a discount rate.

C. MIGRATION RISKS

1. Technical Concerns

The process of properly assessing risk requires an examination of the migration plan from a technical perspective. A strategically sound project does not necessarily mean that technical criteria are being fulfilled. Proposed questions that should be answered when evaluating any systems migration effort include:

- Is the proposed technical solution for migration practical?
- Will the proposed migration path meet all of the current or desired performance needs?

Qualifying a solution as *practical* should require testing the proposed solution against a track record of technological performance. For example, the query response time for a current system such as SeaWatch III should be compared to that of the proposed migratory system. A *practical* system implies that it is achievable. The complexity of operations in a client/server environment must be considered. A proposed migration path may not be practical if there is not adequate expertise or time available to develop and implement the proposed solution. [Ref. 20:p. 65]

a. Schedule

The NRaD plan for migrating ONI systems to the JMCIS architecture calls for the development and implementation of the JMCIS Intelligence and Database Segments to support ONI analysts by mid-1995. This schedule appears somewhat fast-paced given the unproven ability of the proposed distributed system to meet ONI requirements. For example, the SeaWatch III system contains approximately 500,000 lines of code, largely dependent on the IBM mainframe. The bulk of this code is not portable to a UNIX-based platform and must be redeveloped. Furthermore, the SeaWatch III database is several gigabytes in size, and so attempting to replace a system of this size in as little as one year risks the loss of both functionality and system reliability. [Ref. 30]

b. System Performance

Performance of the migratory system is a second potentially high-risk area. Query response time needs to be thoroughly evaluated for the proposed migratory system. Moving the large SeaWatch III system to the TAC-3 distributed environment requires realistic testing under workloads that are representative of the conditions that the system is likely to encounter when implemented. As previously discussed, throughput capabilities remain a major strength of the mainframe. The mainframe has been optimized to support high volume and complex data management with the ability to manage multiple complex tasks. The most advanced and developed desktop systems are just beginning to compete with the mainframe in this area.

c. Database Sizing

The issue of properly sizing the database servers to replace the mainframes is another area of concern. Whether the single processor TAC-3 server is capable of replacing an IBM mainframe seems to require a more thorough analysis. Testing may determine that a multiprocessor configuration will be required to achieve the requirements of the SeaWatch III base system. If so, a more realistic set of cost figures may be needed for decision makers to accurately evaluate the migration plan. This technical decision should be supported with a thorough analysis of the Sea Watch III workload, a realistic set of performance tests, and a careful examination and costing of candidate database servers. Testing should support approximately 25 users simultaneously to determine how a fully-loaded SeaWatch III replacement system will perform. [Ref. 30]

d. System Functionality

As the COE documentation describes, integrating new functionality into JMCIS is conceptually straightforward. One of the first steps is the process of creating a checklist of required functionality. The checklist is used to note what capabilities from JMCIS meet the known functional requirements, what components from JMCIS need further customization, and what new functionality must be developed. However, this step has proven to be easier said than done. Determining the functionality of JMCIS or any new system can be a challenging task for a systems developer. The size and scope of the ONI migration effort with the numerous applications and varying degrees of documented system requirements only serves to further complicate this process. The migration framework presented in this chapter offers an approach to evaluate, based on functionality, migration path alternatives that should be considered for further analysis.

2. Cost Concerns

Proper migration evaluation should include a cost/benefit analysis to summarize the estimated cost associated with the migration plan in sufficient detail to give decision makers the ability to decide whether or not to proceed with the process. As the previous discussion on technical concerns highlighted, many of the technical risks can have further cost affects. With the technical feasibility thoroughly examined, the tangible costs of conversion to and operations in the target environment must be considered. [Ref. 20:p. 79]

a. Conversion Costs

Cost/Benefit analysis must include conversion costs and costs of operating in the new environment. Often the costs associated with conversion are overshadowed by promises of cost savings in a new environment. Up-front conversion costs to distributed systems can represent a sizable investment. Initial estimates indicate the initial conversion of current ONI functionality into the JMCIS Intelligence Segments will cost over $3.5 million. [Ref. 26:p. 11]

b. Operating Costs

Estimating costs of distributed systems requires looking at the significant overhead costs that accompany networked architectures. In general, mainframe-based systems can be classified as capital intensive, whereas the distributed environment is labelled as more labor intensive. Initial estimates indicate that life-cycle costs for the JMCIS environment at ONI will be approximately $640,000 per year. It should be noted that costs of operating in a distributed environment are often grossly underestimated. Personnel support and systems management costs should be thoroughly evaluated to prevent distorted cost estimates. Alternative cost estimates may be required. [Ref. 26:p. 12]

D. A FRAMEWORK FOR MIGRATION EVALUATION

1. The Need for Effective Evaluation

This section will present a framework for evaluating migration path alternatives based on a theoretical structure. The structure for this framework is based on research presented by Captain Daniel Egge, USMC, in his thesis entitled, "A Framework for Evaluating Evolutionary Upgrade Paths of Command, Control, and Communications

Systems." His framework was used to evaluate the upgrade path for the Marine Corps' Tactical Combat Operations (TCO) System with NTCS-A serving as the target system. The structure of his framework has been slightly modified to specifically address migration path evaluation. As previously discussed, this framework could be used for further analysis of migration alternatives that may be presented to ONI as the transition to the JMCIS architecture progresses. The framework is presented to offer decision makers a structured approach to evaluating the migrations options.

One of the most difficult aspects of evaluating information systems is that they will continually change over time, given evolving technologies, standards, and applications. Very few frameworks or methodologies exist that deal specifically with the timing of migration projects, often referred to as the temporal component of information systems. A framework is needed for evaluating the migration paths with specific regard for how the timing aspect of the migration effort will affect the eventual success or failure of the effort as a whole.

Most C4I system procurements today can be viewed as upgrades to existing systems. As discussed, the evolution of Navy C4I systems has been a continual process of upgrades and consolidation of functionality from previous systems. Even large procurements that make sweeping changes will be incremental and evolutionary. Therefore, it is useful to develop a framework for comparing alternative migration paths rather than alternative static information systems. As the path alternatives are often distinguished simply by the temporal component, the timing of the change should be specifically considered. [Ref. 29:p. 37]

2. Defining the Problem

The first step of decision making is to identify and define the problem. Large-scale software development typically involves cost, performance, schedule, and other risk constraints. Theoretical structures often use model development to frame the problem. A mathematical model for the ONI migration effort could be expressed as:

Maximize: **Value**

Subject to: **Costs** $\leq$ **Budget**

This mathematical expression describes the problem's objective with regard for the constraints. The model clearly states the migration effort's objective of maximizing value (functionality) with the migration path chosen, constrained by costs that have some budgetary limit. With the problem clearly defined, the framework for addressing the problem can now be presented.

3. Overview

As presented with the discussion of Navy C4I systems evolution, new information systems are typically procured over time, employing incremental upgrades to keep pace with technology, and migrating functionality into a more technologically capable system. This temporal component of information systems is a difficult aspect to evaluate. Because of the "time value of money," any economic analysis must consider not only how much a proposal will cost, but also when the expenditures will be made and their discounted values. To include this consideration in the analysis, each alternative migration path's life-cycle costs must be expressed in terms of their present value. The framework presented will focus on maintaining functionality while emphasizing the temporal component in evaluating the migration paths toward a goal or target system. [Ref. 29:p. 39]

This framework presents a method that could be useful to the decision makers in making a final decision or in evaluating a potential migration path. The framework is heuristic in nature and should be viewed as a simple procedure for finding a set of feasible solutions when considering alternative migration paths. The framework contains six primary steps:

1. Define the target system's functionality and required technological capabilities.

2. Develop scenarios where the system will be used to the end of the planning horizon and then define a representative set of migration paths from the base system toward the target system within each scenario; each path then becomes a viable candidate path.

3. Develop the discounted (life-cycle) cost for each viable candidate path and identify a set of candidate paths that are budget-feasible. Discounting converts future costs into their equivalent present costs using a discount rate.

4. Develop the discounted value of each budget-feasible path and identify a set of candidate paths that have the greatest value. Values are discounted into their equivalent present values using a discount rate.

5. Determine the expected value of each of the remaining candidate paths with regard for the likelihood of occurrence of each associated scenario. A probability estimate for each scenario is used to adjust greatest value identified in step four and determine an expected value for each path.

6. Select the candidate migration path with the greatest expected value.

Figure 19 summarizes the steps in the framework and will be used in the subsequent discussion.

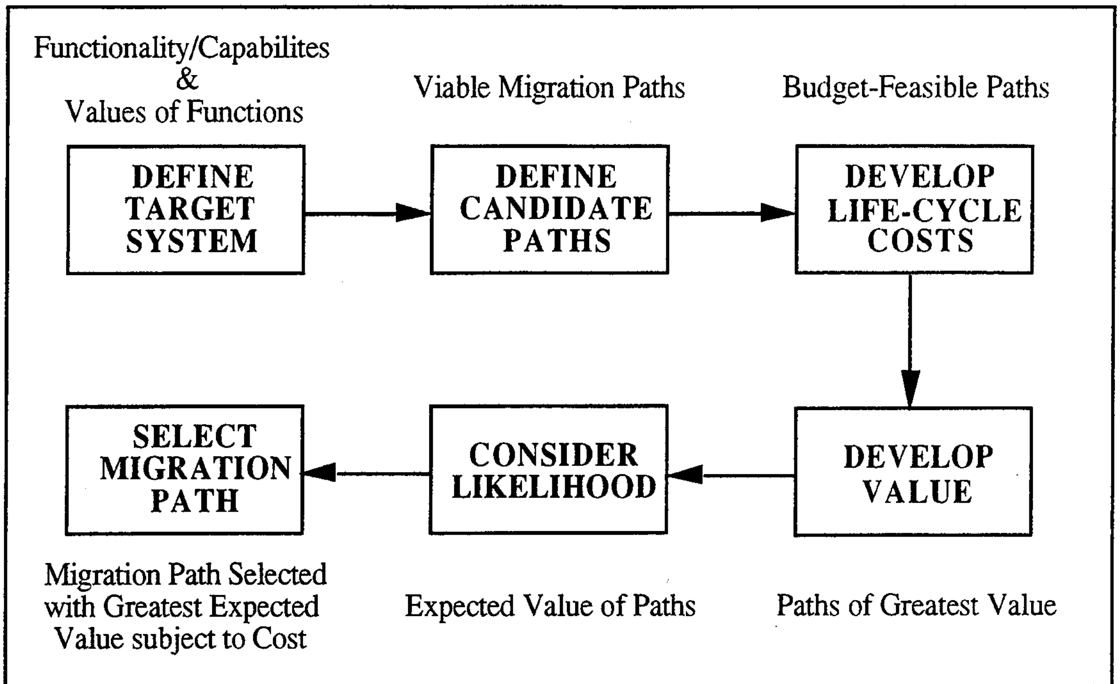

Figure 19: The Steps of the Framework

The first step of the framework defines the target system's functionality in terms of the technological capabilities required to automate each of the required functions. The value of each function is also determined (value will be further discussed). The output of this step is a table showing the relationships between the target system's technological capabilities and the functions it must automate along with the value of each function. [Ref. 29:p. 49]

The second step of the framework begins by characterizing the base system in terms of the technological capabilities. Various scenarios should then be considered with regard for future changes that could affect the migration effort during the planning horizon. For example, potential changes in the functionality requirements and technological capabilities, as well as future budgetary constraints and schedule modifications, should be considered. A representative set of viable paths to the target system that spawn from the base system is then determined for each possible scenario considered over the planning horizon. The output of this step is a depiction of viable candidate paths associated with each scenario.

The third step of the framework involves assigning capability-derived costs to each viable candidate path at discrete time intervals. These costs are then discounted to the present to determine the life-cycle cost of each viable candidate path. Candidate paths that exceed budgetary constraints are then discarded. The output of this step is a set of budget-feasible candidate paths associated with each scenario developed in step two of the framework and a discounted cost determined for each candidate path.

The fourth step of the framework involves assigning functionality-derived values to each candidate path at discrete time intervals. These values are then discounted to the present. The candidate paths with the greatest discounted values are then identified for each scenario. The output of this step is a set of candidate paths that have the greatest discounted values associated with each scenario. Each scenario will have a single candidate path of greatest discounted value.

The fifth step of the framework involves consideration for the likelihood of occurrence of each scenario in order to calculate the expected value of the remaining candidate paths. Probability estimates are made for each scenario. The output of this step is a set of candidate paths that have expected values associated with each scenario based on the likelihood of occurrence.

The final step of the framework involves selecting the candidate path with the greatest expected value. This should result in the identification of a budget-feasible migration path that provides the maximum value.

4. Discussion

A more detailed discussion will now be presented to provide further illustration of the framework. The discussion will provide examples to show application of the framework to the ONI migration effort where possible. Values and costs used in examples are not actual and are included in order to facilitate discussion. Furthermore, only a small sample of functionality and technological capabilities will be used in the discussion. The intent is to simply discuss a framework for example purposes that will provide assistance to further analysis.

a. Define the Target System

The first step of the framework begins by defining the target system's functionality in terms the technological capabilities required to automate each of the required functions. Functions that require automation are usually those functions and key processes that the organization must perform to support the primary mission. Functional decompositions are often useful in this phase. Figure 20 shows a generic functional decomposition. A simple decomposition using an intelligence system, for example, might include production of an intelligence report as the function F1. This function could be decomposed into many lower-level functions represented by F1.1, F1.2, F1.3, and so on. Lower-level functions could include product generation, product output, and office information exchange as required in the production of an intelligence report.

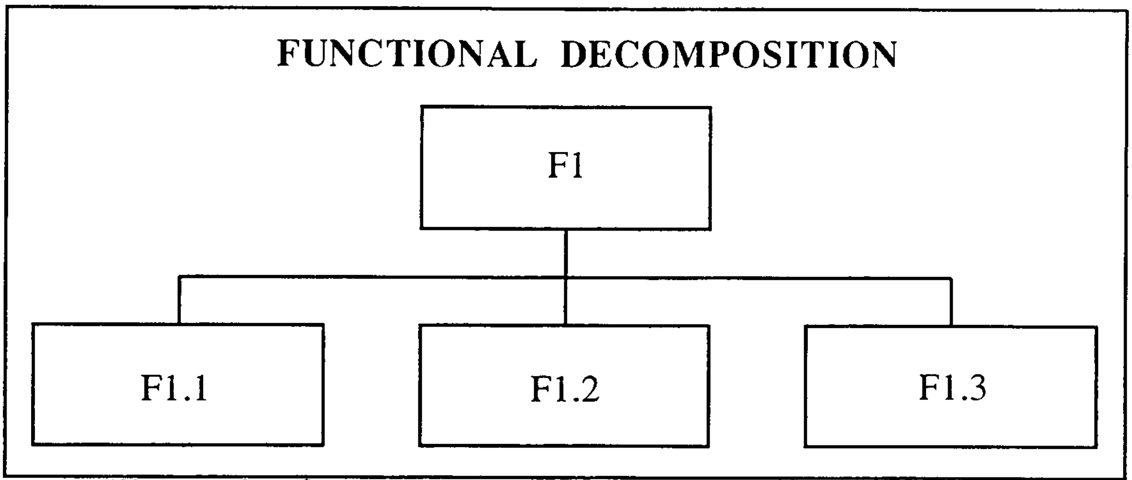

Figure 20: Generic Functional Decomposition [Ref. 29:p. 49]

Once the functions are identified, the technological capabilities required to provide the automated support can be determined. The objective is to obtain a list of capabilities required to automate each function. Technological capabilities required could include text editing, display controls, and LAN connectivity, for example. It should be realized that some of the capabilities identified in the list may not be available yet, given the current state of technology. A functionality/capability matrix can then be constructed that shows the relationship between the functions and the technological capabilities as previously discussed. [Ref. 29:p. 49]

After the relationship between target system functionality and required capabilities is known, the value of each of the functions is then determined. The objective is to assign a value or weight to the functions based on the benefit added to the analysis process when a particular function is automated. One method to accomplish this would be to elicit relative values or the importance of each function from experienced operational experts or analysts. The objective is to recognize the relative importance to the analytical process of automating each target system function. Various methods have been used to elicit these weighted values. System user groups, such as the MerWatch User Group (MUG) at ONI, can be used to define the value of individual functions. Methods such as the Analytical Hierarchy Process (AHP) or the Simple Multi-Attribute Rating Technique (SMART) can provide tools to aid in obtaining relative value or weight of each function. It is important to emphasize that the value should be estimated from the user's perception of the relative importance of a function. [Ref. 29:pp. 51-52]

FUNCTIONALITY / CAPABILITY MATRIX

FUNCTIONS

TECHNOLOGICAL CAPABILITIES

	F1 V1	F2 V2	. . .	Fn Vn
TC1	X			X
TC2	X	X		X
TC3				
TC4		X		X
TC5	X			

Figure 21: Functionality / Capability Matrix with Values Added

The output of this step is a matrix highlighting the relationships between the target system's technological capabilities and the functions it must automate along with the value of each function. Figure 21 illustrates the a functionality/capability matrix with the added V1, V2, . . . Vn to represent the value of that particular function. This matrix could serve as a valuable means of assessing the development effort required for the

JMCIS Intelligence Segment as suggested in the COE documentation. For example, the functions of the Civil Maritime Analysis Segment could be compared to the existing technological capabilities of the JMCIS core software. Assigned values could help prioritize the schedule for the segment development effort.

b. Define Candidate Paths

The second step of the framework begins by characterizing the base system in terms of the technological capabilities. The base system possesses a set of technological capabilities that will be added incrementally over time to eventually fulfill the technological requirements of the target system. Several viable migration paths could be taken. Each path will become a candidate migration path and could be developed by creating a specific scenario of technological change and automation for the base system. As technological capabilities are added to the base system, migratory systems are realized until finally the capabilities of the target system are obtained. [Ref. 29:pp. 54-55]

The migration paths developed will occur over some planning horizon, during which a base system will evolve given the automation opportunities chosen. Various scenarios could occur over this planning horizon that will directly impact the migration effort and the automation opportunities available. For example, potential changes in the functionality requirements and technological capabilities could result from a change in mission orientation and the consumer's intelligence needs. Future budgetary constraints could also pose a greater limitation than expected. Schedule modifications should also be considered with particular regard for the availability of technology, for example. Each scenario foreseen for the planning horizon will have a representative set of viable paths to the target system that spawn from the base system. With these viable paths determined, the output of this step is a depiction of viable migration paths associated with each scenario.

At each discrete time, a viable migration path will have associated with it a set of technological capabilities that have been incrementally added. Each candidate migration path will have a changing list of technological capabilities and a changing list of functions that it can support depending on the discrete time. The next steps in the framework will determine the overall costs and value of each candidate migration path taking into account these changing capabilities.

c. *Develop Life-Cycle Costs*

The third step in the framework involves assigning capability-derived costs to each viable candidate path at discrete time intervals. These costs are then discounted to the present to determine the life-cycle cost of each viable candidate path. The primary objective of this step is to derive a single overall discounted cost for each candidate migration path.

Each candidate path can be viewed as a series of increments that adds technological capabilities. Figure 22 depicts an example breakdown of a candidate path with regard for the time at which a function is automated. The distinction between paths is that some can provide certain capabilities sooner rather than several years in the future. Costs used in this framework are derived from capabilities and are the cost of adding a particular technological capability at some time in the migration path evolution. Costs should include the costs associated with research, development, testing, and evaluation (RDT&E); procurement; and 15 years of operation and support. [Ref. 29:p. 60]

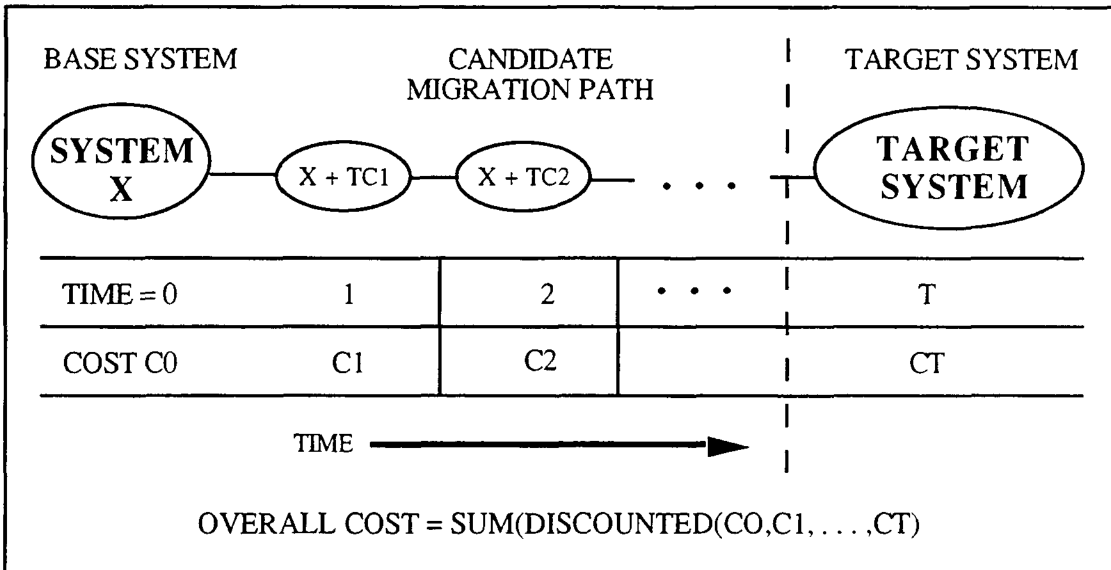

Figure 22: Developing Cost [Ref. 29:p. 56]

The procedure for determining the overall discounted cost of a candidate migration path involves determining when the path will succeed in automating the functions of the target system. Figure 23 provides cost determination for an example migration path using sample estimated cost figures. After determining the discounted costs of the technological capabilities (using a 10 percent discount rate), a single overall discounted cost for each path can be determined. Candidate paths that exceed budgetary constraints are then discarded. The output of this step is a set of budget-feasible candidate paths associated with each scenario with a discounted cost determined for each candidate path.

YEAR	0	1	2	3	4
CANDIDATE PATH	SYSTEM X	X + TC1	X + TC2	X + TC2	X + TC2
FUNCTIONS AUTOMATED	None	None	Mapping	Overlays	None
COST	3500K	400K	207K	207K	100K
DISCOUNT FACTOR	x 1	x 0.955	x 0.868	x 0.789	x 0.717
DISCOUNTED COST	3500K	382K	180K	164K	72K

OVERALL DISCOUNTED COST = 3500 + 382 + 180 + 164 + 72
= **4298K**

Figure 23: Cost of a Candidate Path [Ref. 29:p. 79]

d. Develop Value

The fourth step of the framework involves assigning functionality-derived values to each candidate path at discrete time intervals. These values are then discounted to the present. The primary objective of this step is to derive a single overall discounted value for each candidate migration path. Since the value of each function has been previously determined, the overall value of a candidate migration path depends on the functions it succeeds in automating and when they are automated. The overall value of a candidate migration path is derived by first adding the values of the functions that a set of capabilities automates.

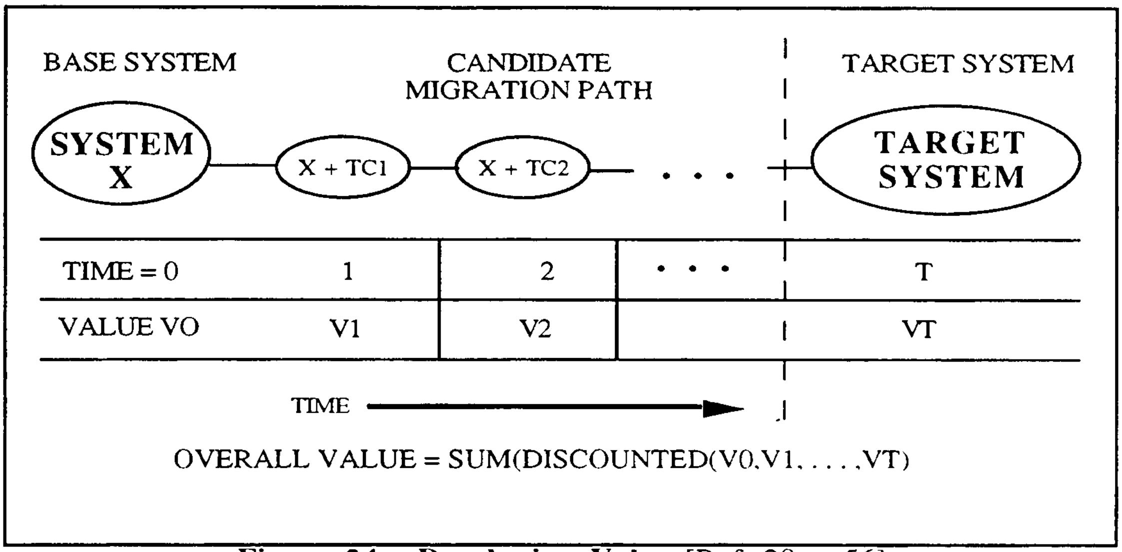

Figure 24: Developing Value [Ref. 29:p. 56]

A previously discussed, each candidate path can be viewed as a series of increments that adds technological capabilities. Figure 24 depicts an example breakdown of a candidate path with regard for the time at which a function is automated. If each candidate path receives the value for a function when it succeeds in automating it, all paths will eventually receive the same value since all candidate paths eventually will reach the capabilities of the target system. Again, one of the distinctions between paths is that some can provide certain capabilities sooner rather than several years in the future. Paths could have other distinctions related to the particular migration path scenario. Other scenarios could include consideration for changes in technology, mission orientation, or political climate. Since the migration effort will occur over some period of time with regard for these various scenarios, a method of discounting the value of added functions must be used. It is generally agreed that the sooner a system can automate a particular function, the more valuable that system will be to the user. A migration path that automates a particular function earlier should receive a greater value. Therefore, if two migration paths are being compared, the path that automates a function sooner, will receive a greater value than a path that automates the function later. This concept of functionality-based value can provide a means of prioritizing the important technological capabilities for migration path selection decisions. [Ref. 29:p. 58-60]

The procedure for determining the overall discounted value of a candidate migration path involves determining when the path will succeed in automating the functions of the target system. Figure 25 provides value determination for an example migration path using weighted values. In this example, the technological capability that automates the mapping function in year two was given a weighted value of two. The overlay was given a weighted value of one. After determining the discounted value of the functions, a single overall discounted value for each path can be determined (using a 10 percent discount rate). The candidate paths with the greatest discounted values are then identified for each scenario. The output of this step is a set of candidate paths that have the greatest discounted values associated one-for-one with each scenario.

YEAR	0	1	2	3	4
CANDIDATE PATH	SYSTEM X	X + TC1	X + TC2	X + TC2	X + TC2
FUNCTIONS AUTOMATED	None	None	Mapping	Overlays	None
VALUE	0	0	2	1	0
DISCOUNT FACTOR	1	0.96	0.87	0.79	0.72
DISCOUNTED VALUE	0	0	1.74	0.79	0

OVERALL DISCOUNTED VALUE = 1.74 + 0.79
= 2.53

Figure 25: Value of a Candidate Path [Ref. 29:p. 79]

e. Consider Likelihood

The fifth step of the framework involves consideration for the likelihood of occurrence of each scenario in order to calculate the expected value of the remaining candidate paths. Probability estimates are made for each scenario. The probability estimate is then used to adjust the overall discounted value of each candidate path. For example, if a particular scenario has a 90 percent likelihood of occurrence, then the overall discounted value for the candidate path of greatest value associated with that scenario would be multiplied by the factor .90. This step results in an expected value for the candidate path derived from the overall discounted value of that path, adjusted for the likelihood of occurrence of each scenario. The output of this step is a set of candidate paths that have expected values associated with each scenario based on the scenario's likelihood of occurrence.

f. Select Migration Path

The final step of the framework involves selecting the candidate path with the greatest expected value. Each scenario will now have associated with it a single budget-feasible migration path with an expected value based on the likelihood of occurrence of that scenario. Selection is based on the candidate path with the greatest expected value. This should result in the identification of a budget-feasible migration path that provides the maximum value to the analysts subject to particular constraints. For this framework, the path that maximizes value subject to cost constraints while reaching the target systems capabilities is the "best" path.

E. SUMMARY AND CONCLUSIONS

The size and scope of the migration effort can vary significantly according to several determinants. The organization's size, culture, and complexity, the current and target architectures, the extent of the change, and the value and cost of the technology will all determine the extent of migration activity required. For some organizations, the migration activity may be minor and may not need to be supported by extensive structure and analysis. For others, the issues of migration will be such that, after analysis, the migration costs and issues will loom large enough that the organization will determine that its best strategy is to delay the migration, at least for the interim, until the costs become less prohibitive. [Ref. 7:Vol. 4,p. V-7]

This chapter presented a method for evaluating a complex migration effort such as that proposed for ONI. The chapter offers a suggested framework to evaluate and select a migration plan. The framework focuses on maximizing value with an emphasis on functionality when scoping the migration problem. This framework could be used for further analysis of migration alternatives that may be presented to ONI as the transition to the JMCIS architecture progresses. Decision makers can apply the structured approach of this framework to evaluated migrations options. Further cost/benefit analysis will be required to make the best use of this framework. As previously presented, "[I]t is difficult enough merely to define--let alone measure--value and cost. Despite these practical difficulties, we can still consider various ways of achieving a reasonable balance between value and cost." [Ref. 31:p. 1]

Migration analysis requires research and validation of the elements of each possible migration solution. The TAFIM Planning Guide offers some typical questions that need to be asked when evaluating a migration proposal:

- Is it viable?
- What products does it need? On what standards are they built?
- When will the products be available?
- What can we do to position for future decisions?
- What education and learning must be undertaken?
- How do we introduce the consequent cultural change? What is the cultural change for development staff, operational staff, users, and management?
- What are the relative costs of each option?
- What benefits are delivered by the option?

[Ref. 7:Vol. 4,p. V-8]

VIII. SUMMARY AND CONCLUSIONS

This thesis has been written primarily for top and middle management at ONI in an effort to demonstrate the process of strategic information systems planning. Strategic information systems planning aligns an organization's information systems with its critical strategic goals and supporting mission-specific functions. The main thrust of this thesis demonstrates the application of established principles of information systems planning to the architectural development effort at ONI. By examining established information systems planning practices, architectural design methodologies, Department of Defense (DoD) guidelines, and published ONI organizational objectives, this thesis guides the reader through the decision-making process involved in strategic IS planning.

The thesis presents a framework for developing a strategically aligned systems architecture specifically applicable to current systems development efforts at ONI. The methodology is structured on guidance provided by the DoD's Technical Architecture Framework for Information Management (TAFIM) Standards-Based Architecture (SBA) Planning methodology. The thesis demonstrates the validity of using the structured architectural approach, presented by the TAFIM and other strategic IS planning concepts, in concert with intelligence-specific IS planning guidance, provided through the DoD Intelligence Information System (DODIIS) program, to systematically address the issues, problems, and critical decisions faced by organizations attempting the strategic IS planning process.

This paper was conceived and written to assist decision makers at ONI as well as systems developers at NRaD. It provides both top-level managers (technical and operational) and potential users (intelligence analysts) at ONI with a breadth of understanding about the Joint Maritime Command Information System (JMCIS) and its role in supporting the strategic vision of ONI, the potential benefits in terms of improved products and services for ONI's intelligence consumers, and the overall benefits to the defense community. Likewise, it offers system developers insight to the users' requirements, providing the perspective of the intelligence analysts as well as the business needs of maritime intelligence. Hopefully, this thesis provides a breadth of understanding that can serve as a vehicle for communication, coordination, and increased understanding among involved parties.

A. STRATEGIC IS PLANNING

This thesis demonstrates a structured approach to strategic information systems (IS) planning that provides a guide for developing an information systems strategy and architecture to support organizational goals outlined in the ONI Strategic Plan. Many companies having strategic IS planning activities agree that planning, set in a strategic framework, allows decision making today that better prepares them for the future. Strategic IS planning must therefore be an integral part of an organization's general planning process and be performed within this strategic framework. [Ref. 3:p. 9]

Strategic IS planning's basic purpose is to link the business and information strategies. The heart of this effort establishes clear IS objectives and expresses them through the organization's IT Principles. Establishing proposed IT Principles through the analysis of ONI's strategic objectives served to initiate the architectural development effort of this research as presented earlier in Chapter III. This key accomplishment guided the planning effort explicitly linked the IT Principles with the opportunities offered by the proposed target architecture as presented in Chapter VI. Ensuring this strategic alignment serves as the key to any strategic IS planning effort and remains essential to the accomplishment of ONI's IT Principles.

B. ARCHITECTURAL OVERVIEW

As introduced in Chapter II, Pressure Point Analysis (PPA) offers a strategic IS analysis technique providing a method to gather and present information focusing on issues of particular interest to management, rather than on the specific technical problems. Pressure Point Analysis provides a simplistically clear analytical approach for planning embodied in four fundamental questions concerning the role of IS in an organization:

- Where are we?
- Why should we change?
- What could we do?
- What should we do?

The display of answers to these questions provides a useful overview to characterize ONI's strategic IS planning process. Figure 24 uses the PPA model to present an overview of ONI's strategic IS planning process and the associated pressures using the PPA model. The following discussion utilizes this model and serves as a review of the structural approach used throughout this thesis.

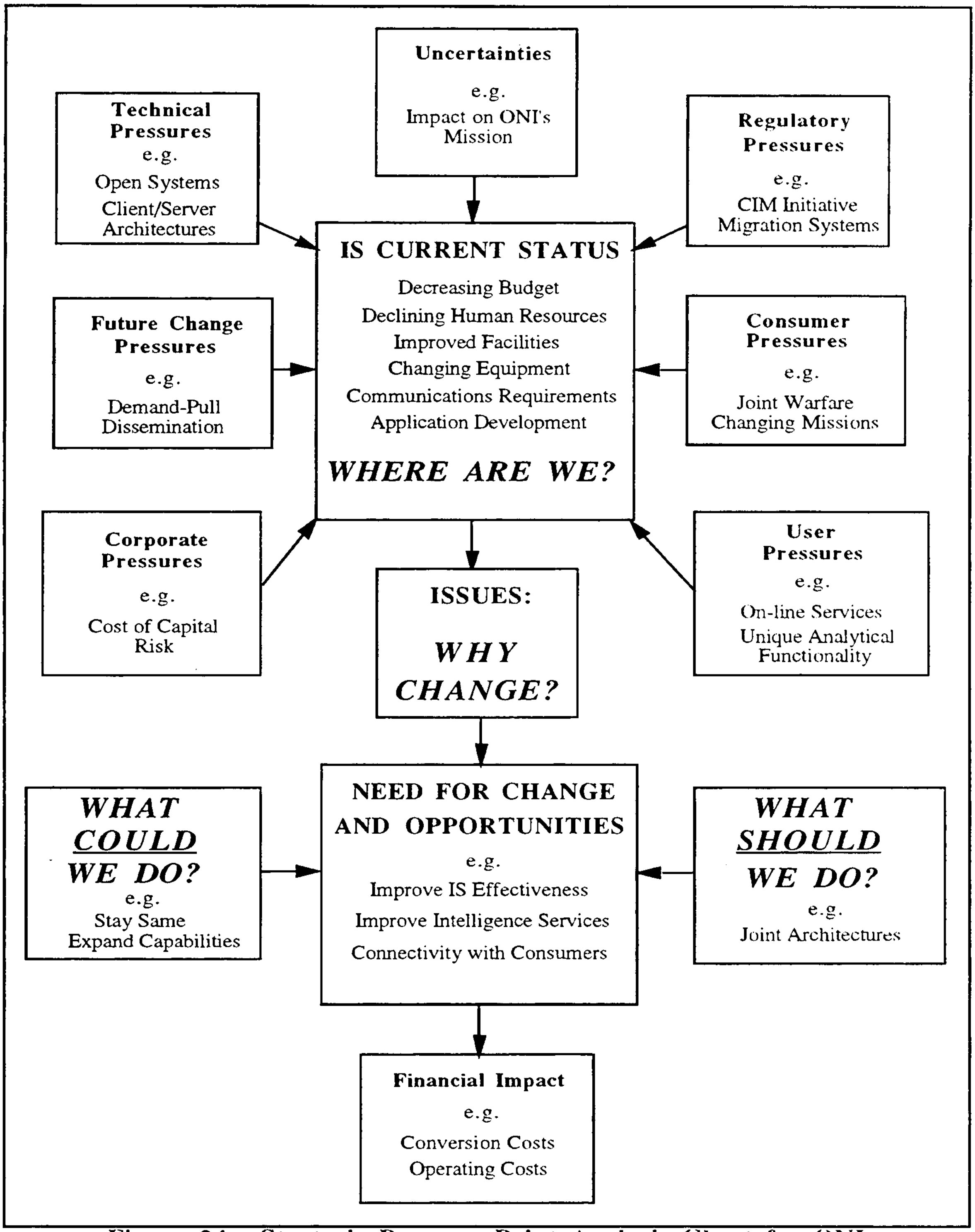

Figure 24: Strategic Pressure Point Analysis Chart for ONI
[Ref. 3:p. 68]

1. Where are we?

Chapter III initiated the structured methodology offered by the architectural approach to strategic IS planning. The chapter presents the issues that initiate the planning process within an architectural framework. The development of initial ONI IT Principles guides the systems development and architectural planning efforts in this phase. Finally, the key issues that impact the overall architecture process are presented to set the stage for further phases in the planning and development process.

Chapter IV presented a high-level baseline characterization of the IS environment currently supporting the critical mission / business functions at ONI. Applications, systems, and databases that directly support ONI intelligence analysts are presented. A management view of the organization focuses on the integration of information and the needs of the organization. The inventory activities of this phase provide key information for migration planning based on the valuation of existing assets and the identification of risk.

2. Why should we change?

Chapter III of this thesis discusses key strategic initiatives, described as "strategic divers," that have provided a vision for information management within DoD. These initiatives directly influence current and future systems development efforts within the Navy and particularly at ONI. Initiatives such as the Corporate Information Initiative (CIM) and *C4I for the Warrior* present the common theme of support to the operational commander through an integrated strategic information management infrastructure and the development of interoperable C4I systems across DoD. Recent C4I systems integration efforts within the Navy reflects the guidance provided by these initiatives.

Recent DoD systems development efforts have received further direction in order to programmatically achieve the goals of the strategic initiatives. All of these directives intend to guide C4I systems development in this era of declining human and financial resources, increasing requirements, and resultant compressing schedules. As these directives indicate, program managers must design, develop, procure, and support affordable systems necessary to meet Naval and joint C4I requirements in view of these constraints. Given that the genesis of the new Global Command and Control System (GCCS) is the Joint Maritime Command Information System (JMCIS), the basis now exists to implement within ONI a truly interoperable, open systems, C4I architecture to support national, theater, and tactical customers.

3. What could we do?

Chapter V presents a draft target architecture to guide systems development and the current evolution at ONI. The chapter specifically presents the Joint Maritime Command Information System (JMCIS) architecture. A thorough understanding of the JMCIS architecture is essential to the architectural development efforts at ONI. Selection of a target architecture must take into account the issues emerging from the baseline phase while addressing the objectives target environment.

Chapter VI builds on the basic understanding of the target architecture by identifying the opportunities presented by JMCIS. The opportunities are presented with regard to the strategic goals and IT Principles of ONI. Opportunities are identified which, once implemented, can demonstrate the value of the architecture and provide immediate benefits to the organization.

4. What <u>should</u> we do?

Finally, Chapter VII presents a framework to assist decision-makers in the process of analyzing a migration path toward the target architecture environment. This chapter specifically addresses concerns regarding the migration plan for ONI systems. It offers a suggested framework for evaluation and selection a migration path. The framework offers decision makers a structured approach for evaluating various migration options.

C. AREAS FOR FURTHER RESEARCH

1. Alternative Architectures

The structured approach of this thesis follows the planning process presented in DoD's TAFIM SBA Planning Guide. Modifications were made where appropriate to fit the process-specific concerns of ONI's architectural development effort. For this reason, the JMCIS architecture was presented without considering alternative infrastructures and was evaluated as the optimum choice. A more typical planning process should examine the question of "What <u>could</u> we do?" by listing strategic alternatives and selecting the best approach. The target architecture development phase should present the alternative approaches.

2. Alternative Migration Options

Similarly, the evaluation of migration requires that the alternative migration strategies are examined to determine the effort, cost, and adequacy of the approach. This requires research and validation of the elements of each possible migration solution. With the ONI migration effort, alternative migration approaches need to be thoroughly scoped.

Chapter VII offers a framework to assist in migration option selection. For example purposes, migration options could be developed to evaluate the effects of implementing the same functionality at different times in the planning horizon.

3. Cost/Benefit Analysis

As suggested in Chapter VII, thorough cost/benefit analysis should be performed before committing resources to new IS projects. Furthermore, a basic principle of economic analysis is to investigate all reasonable alternative methods of satisfying a given objective. When considering a cost/benefit analysis of information systems, the absolute value of both current and future expenditures for the alternatives must be considered. Because of the "time value of money," the cost of each proposed solution must be evaluated with consideration for when expenditures will be made and express each alternative's life-cycle cost in terms of its present value.

D. FUTURE STRATEGIC IS PLANNING CONSIDERATIONS

The objective of strategic IS planning is to define the explicit connection between an organization's business plan and its information systems plan. Strategic IS planning must therefore be an integral part of an organization's general planning process in order to support the organization's goals and objectives.

1. Strategic IS Planning

The success of any strategic planning process requires the support of top management. ONI's Strategic Plan offers considerable regard for the role of information system in the strategic vision of the organization. Continued top-level support is crucial. Strategic IS planning efforts are not likely to succeed without a vision driven from the highest levels of the organization.

2. The Architectural Approach

Possibly the most important role of strategic IS planning is the development of a systems architecture that can be used to successfully guide the organization through a potentially difficult migration. Architecture is not necessarily a diagram of the components or a set of diagrams. Rather, it is a set of strategically aligned policies and guidelines that, when followed, should lead the organization to the desired information systems environment.

LIST OF REFERENCES

1. Emery,J.C., *Management Information Systems-The Critical Strategic Resource,* Oxford University Press, 1987.

2. Director, Office of Naval Intelligence, *Compatibility and Interoperablity of Intelligence Systems*, Memorandum of 10 September 1993.

3. *Strategic and Operational Planning for Informations Systems*, QED Information Services, Inc., 1985.

4. Emery,J.C., *Organizational Planning and Control Systems*, The MacMillan Company, 1969.

5. Targowski,A., *The Architecture and Planning of Enterprise-Wide Information Management Systems,* Idea Group Publishing,1990.

6. McNurlin,B.C., and Sprague,R.H., *Information Systems Management in Practice*, 3rd ed., Prentice Hall,1993.

7. Defense Information Systems Agency (DISA)-Center for Architecture, *Technical Architecture Framework (TAFIM) for Information Management* (Version 2.0), Vol.1-4, 01 November 1993.

8. Chairman, Joint Chiefs of Staff, Joint Pub 1, *Joint Warfare of the US Armed Forces*, 11 November 1991.

9. The Mitre Corporation, *DODIIS Management Board Concept of Operations (CONOPS*), by E.J.Meiers, February 1993.

10. The Mitre Corporation, *Department of Defense Intelligence Information System (DODIIS) Site Transition Methodology*, by J.T.Douglas, October 1993.

11. Office of Naval Intelligence, *Strategic Planning for The Office Of Naval Intelligence: Vision and Direction for the Future*, July 1992.

12. Office of Naval Intelligence, *ONI Strategic Plan.*, June 1993.

13. Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, *Corporate Information Management for the 21st Century - A DoD Strategic Plan*, June 1994.

14. The Joint Staff (J-6), C4 Architecture & Integration Division (J6I), *C4I For The Warrior*, June 1992.

15. Walsh,E.L., "Navy Aims at Joint Opertions Roles and Economies for C4I," *Sea Power*, April 1994.

16. Copernicus Project Team, *The Copernicus Architecture, Phase I Requirements Definition.*

17. Dearborn,R.D. and R.C. Morales, *An Overview of the Copernicus C4I Architecture*, Master's Thesis, Naval Postgraduate School, Monterey, California, March1992.

18. The Joint Staff (J-6), C4 Architecture & Integration Division (J6I), *C4I For The Warrior*, June 1993.

19. Assistant Secretary of Defense - Command, Control, Communications, and Intelligence, *Detailed Selection Criteria for C3I Migration Systems*, Memorandum of 13 December 1993.

20. Hutson,P.M., *Downsizing Information Systems: Framing the Issues for the Office of Naval Intelligence (ONI)*, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1994.

21. Naval Education and Training Command, *Fundamentals of Naval Intelligence*, Training Manual, Naval Education and Training Command Management Support Activity, March 1990.

22. J.G. Van Dyke & Associates, Inc., *ONI Local Area Network Architecture and Baseline*, 12 March 1993.

23. Inter-National Research Institute,Inc., *Joint Maritime Command Information System (JMCIS) Common Operating Environment (COE)*, Rev 1.4, February 1994.

24. Guass,J.A., RADM, USN, "Navy Command Systems Strategy for the 1990s," Briefing, 07 December 1993.

25. Fernandes,K., *User Interface Specifications for the Joint Maritime Command Information System (JMCIS)*, Space & Electronic Warfare Systems Command, Washington, D.C., November 1993.

26. Naval Command, Control, and Ocean Surveillance Center (NCCOSC), Research, Development, Testing, and Evaluation Division (NRaD), *Draft Program Management Plan for JMCIS Migration of ONI Systems*, 24 June 1994.

27. Naval Command, Control, and Ocean Surveillance Center (NCCOSC), Research, Development, Testing, and Evaluation Division (NRaD), *Compatibility and Interoperability of Intelligence Systems*, Draft Message, April 1994.

28. Chadwick,D.L., COL, USMC, Commanding Officer, Marine Corps Tactical Systems Support Activity (MCTSSA), *The Marine Corps Strategy to the Global Command and Control System Core Services*, Briefing, 28 February 1994.

29. Egge,D.Q., *A Framework for Evaluating Evolutionary Upgrade Paths of Command,Control, and Communications Systems,* Master's Thesis, Naval Postgraduate School, Monterey, California, June 1993.

30. Office of Naval Intelligence, *ONI Migration to JMCIS: Alternate Approaches and Opportunities*, Draft Briefing, Systems Directorate (ONI-7), June 1994.

31. Emery,J.C., "Cost/Benefit Analysis of Information Systems," *Fundamentals of Computer-Based Management Information Systems*, Addison-Wesley, 1973.

32. Space and Naval Warfare Systems Command (SPAWAR), *Navy Tactical Command System -Afloat (NTCS-A) Project Overview*, brief given on 13 July 1993.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6415	2
2.	Library Code 52 Naval Postgraduate School Monterey, California 93943-5000	2
3.	CAPT Richard Gragg Deputy, Systems Directorate (ONI-7B) Office of Naval Intelligence 4600 Silver Hill Road Washington, D.C. 20389-5000	1
4.	Mr. Bob Wilson Deputy, Civil Maritime Analysis Department (ONI-21) Office of Naval Intelligence 4600 Silver Hill Road Washington, D.C. 20389-5000	1
5.	LCDR Nancy Clark Head, AIS Operations Department (ONI-74) Office of Naval Intelligence 4600 Silver Hill Road Washington, D.C. 20389-5000	1
6.	Mr. Maurice Deschenes Systems Directorate (ONI-72) Office of Naval Intelligence 4600 Silver Hill Road Washington, D.C. 20389-5000	1
7.	Dr. Richard Jaffee, Code 421 Deputy for Business, Command and Intelligence Systems Division RDT&E Division (NRaD) Naval Command Control Ocean Surveillance Center 49275 Electron Drive San Diego, CA 92152-5000	1
8.	CAPT(Ret.) R. Norman Channel Naval Postgraduate School Code NS/CH Monterey, California 93943-5000	1

9. CDR Peter R. Hull 1
Naval Postgraduate School
Code NS/HL
Monterey, California 93943-5000

10. Dr. James C. Emery 1
Naval Postgraduate School
Code SM/EY
Monterey, California 93943-5000

11. Dr. Carl R. Jones 2
Naval Postgraduate School
Code SM/JS
Monterey, California 93943-5000

12. Dr. Dan C. Boger 1
Naval Postgraduate School
Code SM/BO
Monterey, California 93943-5000

13. Dr. Mike Sovereign 1
Naval Postgraduate School
Code CC/SM
Monterey, California 93943-5000

14. Dr. Orin Marvel 1
Naval Postgraduate School
Code CC/MA
Monterey, California 93943-5000

15. LT Bruce F. Loveless 1
COMUSNAVCENT (N2)
FPO AE 09501-6008