NAVAL POSTGRADUATE SCHOOL
Monterey, California
THESIS

IMPLEMENTATION OF INFORMATION ASSURANCE RISK MANAGEMENT TRAINING INTO EXISTING DEPARTMENT OF THE NAVY TRAINING PIPELINES

by

Matthew J. Labert

March 2002

Thesis Advisor:	Rex Buddenberg
Second Reader:	Steven Iatrou

Approved for public release; distribution is unlimited.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
29 Mar 2002	N/A	-

Title and Subtitle Implementation of Information Assurance Risk Management Training into Existing Department of the Navy Training Pipelines	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Labert, Matthew	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Naval Postgradaute School Monterey, California	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 141	

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Implementation of Information Assurance Risk Management Training into Existing Department of the Navy Training Pipelines			**5. FUNDING NUMBERS**
6. AUTHOR(S) Labert, Matthew J.			
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)			**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**

13. ABSTRACT ***(maximum 200 words)***

With the implementation and continuing research on information systems, such as Information Technology for the 21st Century (IT-21), Navy-Marine Corps Intranet (NMCI), and "Network-Centric warfare," there is little doubt that the Navy is becoming heavily dependent on information and information systems. Though much has been accomplished technically to protect and defend these systems, an important security issue has thus far been overlooked—the human factor.

Information Assurance Risk Management (IARM) was a proposal to standardize the way DON personnel discuss, treat, and implement information assurance. IARM addresses the human security aspect of information and information systems in a regimented way to be understandable through all levels of the DON.

To standardize the way DON personnel perceive information assurance, they must be taught what IARM is and how to use it. Can an IARM course be implemented in the DON, and if so at what level and to whom should it be taught?

14. SUBJECT TERMS Training, Information Assurance (IA), Information Assurance Risk Management (IARM)			**15. NUMBER OF PAGES** 141
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 **Standard Form 298 (Rev. 2-89)**

Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

IMPLEMENTATION OF INFORMATION ASSURANCE RISK MANAGEMENT TRAINING INTO EXISTING DEPARTMENT OF THE NAVY TRAINING PIPELINES

Matthew J. Labert
Lieutenant, United States Navy
B.S., United States Naval Academy, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2002

Author:
Matthew J. Labert

Approved by:
Rex Buddenberg, Thesis Advisor

LCDR Steven Iatrou, Second Reader

Dr. Dan Boger, Chairman,
Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

With the implementation and continuing research on information systems, such as Information Technology for the 21st Century (IT-21), Navy-Marine Corps Intranet (NMCI), and "Network-Centric warfare," there is little doubt that the Navy is becoming heavily dependent on information and information systems. Though much has been accomplished technically to protect and defend these systems, an important security issue has thus far been overlooked—the human factor.

Information Assurance Risk Management (IARM) was a proposal to standardize the way DON personnel discuss, treat, and implement information assurance. IARM addresses the human security aspect of information and information systems in a regimented way to be understandable through all levels of the DON.

To standardize the way DON personnel perceive information assurance, they must be taught what IARM is and how to use it. Can an IARM course be implemented in the DON, and if so at what level and to whom should it be taught?

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. PURPOSE OF RESEARCH 1
B. RESEARCH QUESTIONS 2
1. Primary: 2
2. Subsidiary: 2
C. SCOPE, LIMITATIONS, AND ASSUMPTIONS 2
D. THESIS ORGANIZATOIN 3

II. WHY INDOCTRINATE INFORMATION ASSURANCE RISK MANAGEMENT 5
A. THE TRADITIONAL APPROACH TO INFORMATION ASSURANCE 5
1. Space and Naval Warfare (SPAWAR) Systems Command 7
2. Fleet Information Warfare Center (FIWC) and Network Operation Centers (NOC) 10
3. Afloat Networks 11
4. A Confused Organization 11
B. INTRODUCTION TO INFORMATION ASSURANCE RISK MANAGEMENT 13
C. PRINCIPLES 13
1. Accept No Unnecessary Risk 13
2. Make Risk Decisions at the Appropriate Level 14
3. Accept Risk When Benefits Outweigh the Costs 15
4. Anticipate and Manage Risk by Planning 15
D. BENEFITS 16
1. Manages Information Assurance Risks 16
2. Increases the Level of Information Assurance 17
3. Identifies Information Assurance Assets, Procedures, and Risks 18
4. Provides Cost-effectiveness and Efficiency 19
5. Standardizes Information Assurance Training 20
E. SUMMARY 20

III. TRAINING 21
A. DEVELOPING A COURSE—TRAINING PROJECT PLAN (TPP) 21
1. Justification for Course Development 23
2. Impact Statement 25
3. Mission Statement 25
4. Further Requirements 26
B. LEVELS OF INSTRUCTION 27
1. Training 27
2. Education 27
3. Semantics 28
C. WHO NEEDS TO KNOW 28
1. Officers 29
a. The Designator/Grade 30

b. The Navy Officer Billet Classification (NOBC) ... 31
c. Sub-specialty Codes ... 31
d. The Additional Qualification Designation (AQD) ... 31
e. Illustration of NOOCS In a URL Junior Officer ... 32
f. Senior Decision Makers ... 34
g. Information Professionals ... 35
2. Enlisted Personnel ... 37
a. Applicable Rates ... 38
b. Applicable Billets/Positions ... 41
c. Users and Supporters ... 44
3. Putting it all together ... 48
D. IMPLEMENTING IARM INTO IT "A" SCHOOL ... 50
1. Course Skills and Training ... 51
2. Specific Skills and Knowledge to be Acquired for the IARM Topic ... 52
3. Organization of Subject Matter ... 53
4. Developer's Intent with Respect to the Course and Each Unit of Instruction ... 54
5. Lesson Plans ... 59
a. Topic 3.1: Introduction to Information Systems Security (INFOSEC) ... 59
b. Topic 3.2: Introduction to IARM ... 60
E. SUMMARY ... 61

IV. CONCLUSIONS ... 63
A. SUMMARY ... 63
B. RECOMMENDATIONS ... 64
1. Pilot Program ... 64
2. New Ideas on Training ... 65
C. FUTURE AREAS OF STUDY ... 66
1. Naval Education and Training Command Course Requirements ... 66
2. Pilot Program Study ... 66
3. IARM in the Department of Defense and the Civilian World ... 67
D. FINAL COMMENTS ... 68

APPENDIX A. NAVY INFORMATION ASSURANCE (IA) PROGRAM ... 71

APPENDIX B. INFORMATION ASSURANCE RISK MANAGEMENT PROCESS (HERNANDEZ P. 41-47) ... 91
E. IARM PROCESS ... 91
1. Identify Vulnerabilities ... 91
2. Asses Vulnerabilities ... 92
3. Make Risk Decisions ... 95
4. Implement Controls ... 96
5. Supervise ... 97

APPENDIX C. PROPOSED INFORMATION ASSURANCE RISK MANAGEMENT (IARM) CURRICULA (HERNANDEZ, P. 69-75) ... 99
A. INDOCTRINATION TRAINING OUTLINE ... 102

B. USER OUTLINE 103
C. INFORMATION TECHNOLOGY SUPPORT CORPS OUTLINE 104
D. INFORMATION TECHNOLOGY (IT) OFFICER CORPS OUTLINE 105
E. SENIOR LEADERSHIP OUTLINE 105

APPENDIX D. OPERATIONAL RISK MANAGEMENT (ORM) OPNAV INSTRUCTION 3500.39A 107

GLOSSARY OF TERMS 113

LIST OF REFERENCES 119

INITIAL DISTRIBUTION LIST 121

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 2-1. DoN IA Organization Chart. 12
Figure 3-1. Curriculum Development Process (From: NAVEDTRA 131A p.1-5). 23
Figure 3-2. Current DoN Network Concerns. (From: VADM Mayo Information Professionals presentation)..... 24
Figure 3-3. "The Network After Next" (From: VADM Mayo Information Professionals presentation). 26
Figure 3-4. "Aligning for the Warfare Domain" (From: VADM Mayo Information Professionals presentation)..... 37
Figure 3-5. Sample EDVR (From: Surface Warfare Officer Schools Command)..... 43
Figure 3-6. "Manning Documents" (From: Surface Warfare Officer Schools Command). 49
Figure B-1. "IARM Risk Assessment Code Chart (After U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)" (From: Hernandez p. 43) 93
Figure B-2. "The Cyclic IARM Process (After U.S. Air Force ORM Process)" (From: Hernandez p. 47) 98

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 2-1. DoN IA Objectives (From: CNO N643 p. 2-3). 6
Table 2-2. "IARM vs Traditional Approach" (From: Hernandez p. 51)..... 17
Table 3-1. "Career Path After Recruit Training" (From: "Information Systems Technician (IT)")..... 51
Table 3-2. IT "A" School Computer/Network Curriculum (From: "Information Systems Technician 'A' School"). 56
Table 3-3. "Introduction to Information Systems Security (INFOSEC)" Breakdown (From: "Information Systems Technician 'A' School"). 57
Table 3-4. Proposed "Unit 3" with integrated IARM Topics. 58
Table B-1. "Assets and Security Services (After Pfleeger)" (From: Hernandez p. 42)..... 92

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

AQD	Additional Qualification Designation
CO	Commanding Officer
COMMO	Communications Officer
DoN	Department of the Navy
DoD	Department of Defense
EDVR	Enlisted Distribution and Verification Report
IA	Information Assurance
IARM	Information Assurance Risk Management
IIS	Institute for Information Security
IP	Information Professional
IS	Information System
ISD	Information Systems Design/Development
ISO	Information Systems Operations
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
IT-21	Information Technology for the 21st Century
LPD	Low Probability of Detection
LPI	Low Probability of Interception
NEC	Navy Enlisted Classification Code
NMCI	Navy-Marine Corps Intranet
NMP	Navy Manning Plan
NOBC	Navy Officer Billet Classifications
NOOCS	Navy Officer Occupational Classification System
NPS	Naval Postgraduate School
OCDR	Officer Distribution and Control Report
OIC	Officer-in-Charge
OPS	Operations Officer
ORM	Operational Risk Management
POE	Projected Operational Environment
RAC	Risk Assessment Code
ROC	Required Operational Capabilities
SSP	Subspecialty Code
SWO	Surface Warfare Officer
XO	Executive Officer

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to recognize certain people without whom this thesis would not have been possible. First and foremost is my loving wife, a person of endless patience, ceaseless knowledge, and limitless support. Thank you to family and friends for your encouragement; to Professor Rex Buddenberg and LCDR Steven Iatrou for guidance on thesis topics and advising on the thesis; and to LCDR Ernest Hernandez for deriving IARM in the first place. Also extended is my gratitude to the United States Navy who has given me extraordinary opportunities, including the continuation of my education here at the Naval Postgraduate School.

I would also like to acknowledge "the One who holds the future," whose plan is more perfect than I could have ever expected.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE OF RESEARCH

Information Assurance Risk Management (IARM) has been proposed by LCDR Ernest Hernandez as a method to standardize the Department of the Navy (DoN) human factors involvement in information assurance (IA) (Hernandez p. 29). Because information assurance is vital to the DoN, as determined by the Chief of Naval Operations in Chief of Naval Operations Instruction (OPNAVINST) 5239.1B, the need for IA training becomes evident. If the proposed IARM method will best satisfy the CNO's requisite (See Chapter 2) for IA training, then IARM education and training is a requisite. This thesis accepts both the problem identified and the solution proposed by LCDR Hernandez and proceeds from there.

If IARM training and education is a requisite, then to whom should it be taught? The DoN has numerous programs and systems for which IARM would be applicable. However, because the applicable programs and systems are many, there exist a copious number of personnel to be trained. Skills, knowledge, rank, and job specialty vary greatly among these personnel. With such immense involvement of a multiplicity of DoN personnel, how can IARM be effectively taught to specific personnel?

The answer lies within the roots of IARM itself. IARM evolved from the Operational Risk Management (ORM), of which former Chief of Naval Operations (CNO) Admiral Jay Johnson said, "ORM applies across the entire spectrum of naval activities, from joint operations and fleet exercises to daily routine. We must encourage top down interest in the ORM process, from the flag level all the way down to the deck plates." To be applicable Navy-wide, IARM, like its ORM cousin from which it was

derived, must also be "applied across the entire spectrum of naval activities." Therefore, IARM should also be encouraged and taught from the "flag level all the way down to the deck plate."

B. RESEARCH QUESTIONS

1. Primary:

Can an Information Assurance Risk Management module/course be implemented into existing DoN training pipelines to standardize the human factors involvements in Information Assurance Navy-wide?

2. Subsidiary:

If an IARM module/course can be implemented in the DoN, then it is obligatory to address the following questions:

a. Who would benefit from this course?
b. At what level(s) should this course be taught?

C. SCOPE, LIMITATIONS, AND ASSUMPTIONS

IARM was proposed and developed by LCDR Hernandez. This research does not intend to re-define IARM, but to accept LCDR Hernandez conclusions and examine the possibilities of implementing IARM training. Though certain key concepts of IARM are readdressed, the reader should become familiar with LCDR Hernandez's thesis on IARM. (See Bibliography.)

The primary and subsidiary research questions are not intended to focus specifically on the content of an IARM course. In fact, an IARM course content cannot be specifically addressed, until the questions of whether or not there is necessity and a

requisite for the course, what is the appropriate level for the course, and to whom the course should be taught are answered first. LCDR Hernandez's work started to address, but never fully answered these essential questions (see Appendix B). Though the curricula itself is not the focus of this thesis, IARM course specific information is alluded to, in order to fully develop the answers to the preliminary and subsidiary research questions.

Although IARM is useful to the entire DoN, the training of DoN civilian personnel is not addressed. In addition, the DoN is comprised of numerous communities and specialties, not all community specific applications of IARM are addressed. The author is most familiar with the Surface Warfare Community (SWO); a majority of the examples and applications of IARM and DoN training pipelines are addressed from the SWO perspective. This does not necessarily imply that other DoN communities are not addressed in this thesis, and certainly does not preclude IARM from being used or taught in other DoN communities.

Though changes are proposed by this research, these changes are not fundamental to existing training pipelines.

D. THESIS ORGANIZATOIN

Chapter I discusses the purpose and area of research, the research questions to be addressed, and the scope and methodology used to conduct the research. Definitions and abbreviations are also listed in Chapter I.

Chapter II briefly reviews the IARM concept and discusses why IARM is useful to the DoN. The IARM process is briefly discussed to familiarize the reader with the IARM method and illustrate its ease of use.

Chapter III examines the feasibility of an IARM course/module for the DoN and attempts to answer the primary research question. The subsidiary research questions are also addressed in this chapter, specifically as to what level and to whom an IARM course should be taught.

Chapter IV contains a summary of the thesis, conclusions, recommendations, and further areas of research are presented.

Appendix A is the governing Information Assurance instruction for the DoN from the Chief of Naval Operations. It is included as background information for IA, and is used to establish the requisite for IARM training.

Appendix B is an excerpt from LCDR Hernandez IARM thesis, included to fully develop the IARM concept and to assist the reader in fully understanding how to use IARM process.

Appendix C is another excerpt from LCDR Hernandez IARM thesis. A tentative IARM curricula and general corresponding levels of instruction were proposed.

Appendix D is the Operational Risk Management (ORM) instruction from the Chief of Naval Operations. It demonstrates DoN commitment to risk management, and illustrates to what degree the DoN should go in adopting IARM.

II. WHY INDOCTRINATE INFORMATION ASSURANCE RISK MANAGEMENT

If as one people speaking the same language they have begun to do this, then nothing they plan to do will be impossible for them.

-Genesis 11:6

A. THE TRADITIONAL APPROACH TO INFORMATION ASSURANCE

The Department of the Navy's current approach to IA is governed by the Chief of Naval Operations Instruction (OPNAVINST) 5239.1B, Department of the Navy Information Assurance Program. Table 2-1 outlines the IA objectives stated in OPNAVINST 5239.1B. Derived from this single instruction are a series of Naval Publications (5239 series) that break down specific areas of IA even further. Pub 01 is intended to introduce and summarize the DoN's approach to IA and "…foster a common understanding of IA principles, concepts and interrelationships among system planners, organizational managers, Information Systems Security Officers and Managers, and users" (OPNAVINST 5239.1B). However, under this instruction, IA is broken down into several modules: Information Security (INFOSEC), Operation Security (OPSEC), Communications Security (COMSEC), Monitoring, and Vulnerability Assessments (CNO N643 p. 1). Although Pub 01 attempts to foster a "common understanding" and lay the groundwork for a layered defense for IA, it necessitates the need for thirty-five additional 5239 modules that provide directed guidance for specific areas of IA. Although several of these modules still target a general audience (e.g., Network Security Managers, System Administrators, users, etc.), a number of them are "area" specific.

DoN IA Objectives
➢ Employ efficient procedures and cost-effective, information-based security features on all Information Technology (IT) resources procured, developed, operated, maintained, or managed by DoN organizational elements to protect the information on those resources.
➢ Protect the confidentiality, integrity, availability, authenticity, and non-repudiation of information and resources to the degree commensurate with their value, as determined by the required level of IA, classification or sensitivity level and the consequences of their exploitation or loss for a period required by the mission supported.
➢ Conduct an assessment of threats, identify the appropriate combination of safeguards from the IA disciplines, and apply an appropriate Certification and Accreditation (C&A) process for each specific information system developed by a program office and for each local site employing networks and deployed information systems.
➢ Adopt a risk-based life cycle management approach in applying basic minimum uniform standards for the protection of DoN information technology resources that produce, process, store, or transmit information.
➢ Establish standardized IA training within the DoN.

Table 2-1. DoN IA Objectives (From: CNO N643 p. 2-3).

The fact that thirty-five modules were needed to address different aspects of IA also alludes to another important DoN distinction between "general audiences" (i.e., users) and "specific communities" (i.e., those responsible for technical support). Though it is necessary to understand the differences amongst users and technical supporters involved in IA, it does little for the standardization of training to compartmentalize requisite IA knowledge into two seemingly disconnected groups and thirty-five publications.

The IA Pub 5239 modules are intended to provide a common understanding of IA principles, concepts, and interrelationships based on the DoN IA objectives. Through this "common understanding," it was envisioned that the modules could then be used to assist in planning and securely operating information systems and to help system users maintain security awareness. However, with so many modules and only certain modules applying to certain people, how does the DoN achieve a "common understanding" of IA as a whole?

One of the major challenges faced by the DoN IA program is how to change its stand-alone security systems to an integrated, or "defense-in-depth," security strategy that supports an overall IA doctrine. The DoN recognizes that part of the doctrine must "…be accomplished through the employment of defensive layers that include the IA disciplines" (CNO N643 p. 5). This appears to be a good start, but herein also lies the largest problem—"IA disciplines". Currently splintered organizations focus on individual IA disciplines that address specific IA objectives. What the DoN needs, is a governing IA doctrine that aligns the numerous fractured IA organizations into a common IA goal that truly provides a "defense-in-depth" security strategy.

1. Space and Naval Warfare (SPAWAR) Systems Command

The commander of SPAWAR (COMSPAWARSYSCOM) is designated by OPNAVINST 5239.1B as DoN IA program manager (PMW-161). As IA program manager, COMSPAWARSYSCOM is responsible for drafting and maintaining a master plan for the Navy consisting of "…identification and formal documentation of IA goals and objectives for the Navy, a strategy for achieving those goals and objectives, a description of IA programs, projects and initiatives that will result in the capabilities

needed, and an IA risk management plan" (OPNAVINST 5239.1B). Specifically, PMW-161 is "…*dedicated to protection* of United States Navy information *systems* afloat and ashore" ("Mission") [emphasis added]. Although SPAWAR is tasked with overall management of the Navy's IA program through PMW-161, it is clear to see from its tasking that SPAWAR's direct involvement is more of a technical nature (i.e., unlike the NNOC, SPAWAR is not involved with people or personnel management).

SPAWAR's self-describing mission is to "…provide the warfighter with knowledge superiority by *developing, delivering, and maintaining* effective, capable and integrated command, control, communications, computer, intelligence and surveillance systems," and to "…provide *information technology* and space systems for today's Navy and Defense Department activities while *planning and designing* for the future" ("Mission") [emphasis added]. SPAWAR's technical focus is still in accordance with OPNAVINST 5239.1B, which also designates SPAWAR as the technical lead for IA and tasks it with providing "…systems and security engineering and integration testing and support for Navy information systems and networks with IA requirements." Furthermore it is to "…maintain a Navy IA research and development program to ensure maximum and smooth transition of new technologies to operating forces, fully integrated for maximum cost effectiveness with existing technologies" (OPNAVINST 5239.1B)

Though tasked as the overall program manager for IA, it is evident that SPAWAR is more focused on an IA technology objective than overall security. Even with a technology-based focus, SPAWAR neglects the other IA objectives directly impacted by its own technology. Even with its main focus on technology, there still does not exist an

overall IA technology strategy, as SPAWAR is not the only organization concerned with IA.

Within SPAWAR, PMW-165 is the program manager responsible for the technical aspect of "afloat computer networks" ("PMW-165 Home Page"). Its assigned mission is to provide "the implementation of an integrated, interoperable network infrastructure, basic network and information distribution services, and full Information Technology afloat," which it accomplishes by supplying "technical, engineering, planning, design, installation and life cycle support of afloat Local Area Networks (LANs), Basic Network and Information Distribution Services (BNIDS), and hardware and software required for full User IT support" ("PMW-165 Home Page").

Although PMW-165 is directly tasked with afloat-networks technology, and therefore indirectly with afloat-IA, there are still numerous afloat-IA-technology crossovers that do not fall under PMW-165's (or any other SPAWAR programs) purview. On a single ship, for example, there may exist network components installed under the ship's own prerogative, installed by another organization (e.g., NAVSEA) or, in the case of amphibious ships, installed by embarked Marine Corps personnel. (Consequently, while Marine Corps networks must be interoperable with their Navy counterparts, Marine Corps IA does not fall under the guidance of OPNAVINST 5239.1B.) Most importantly, most IA issues are end-to-end, meaning that a portion of the infrastructure is ashore. Even though PMW-165 shares responsibility for afloat-network technology, the ship itself is a node in a much larger network (other ships and shore-based installations), which fall under the purview of PMW-161 and other programs such

as Information Technology for the 21st Century (IT-21), Navy-Marine Corps Intranet (NMCI), which again, are not necessarily directly accountable to SPAWAR.

2. Fleet Information Warfare Center (FIWC) and Network Operation Centers (NOC)

The Fleet Information Warfare Center and the Naval Computer Incident Response Team (NAVCIRT), which it manages, are tasked with computer network defense, which also entails IA security. Tasked by OPNAVINST 5239.1B, FIWC provides "…assistance [in coordination with PMW-161] in identifying, assessing, containing, and countering incidents that threaten Navy information systems and networks." FIWC and NAVCIRT offer anti-virus scanners, computer security toolboxes (designed by SPAWAR), guidance for system configuration changes (made on systems designed and installed by SPAWAR), and provide security information to DoN activities via computer security advisories that "contain current vulnerability announcements on various systems…" ("Mission, Vision And Guiding Principles"). In addition to their focus on the DoN system-security objective, FIWC and NAVCIRT also accomplish the certification and accreditation (C&A) objective for afloat-networks.

Another organization that partially addresses the system-security objective, as well as portions of the information-security objective, is the Network Operation Center (NOC). Though not directly tasked by OPNAVINST 5239.1B to provide IA, Fleet NOCs are able to do so by acting as a gateway for the ship-shore and shore-ship interface for Navy networks. This single point interface allows the NOC to perform basic IA services including firewall protection, intrusion detection, and virus scanning of e-mail attachments for ships at sea ("Information Technology Presentation for the 21st Century").

3. Afloat Networks

Although other organizations share varying degrees of IA responsibilities, and attempt to meet different IA objectives, the individual CO is ultimately responsible for all aspects of information and information systems in a single command. According to OPNAVINST 5239.1B, "…the commanding officer (CO), commander, or officer-in-charge (OIC) are [sic] responsible for overall management of IA at the command level." Although the commander retains responsibility, he is directed to appoint an Information Systems Security Manager (ISSM) or Information Systems Security Officer (ISSO) to assist in management and administration for the organization. In addition to being responsible for the ship's IA, it is also important to note that the CO is also given the responsibility to "…make sure standard IA operating procedures are available and used," "…IA awareness indoctrination training and indoctrination is performed," and "…all personnel performing IA functions receive initial basic and system specific training" (OPNAVINST 5239.1B).

In the end, it is the CO and the ISSM who are responsible for incorporating all aspects of the IA policy. Though numerous organizations like SPAWAR, FIWC, NAVCIRT, and the Fleet NOCs provide assistance in different IA objectives, no one entity, other than the CO, integrates all of the IA objectives. It is also important to note that while the individual organizations are IA "technical supporters," and probably the IA experts, the sole embodiment of the IA policy is little more than a responsible IA "user."

4. A Confused Organization

The DoN understands the importance of IA but, by simply examining parts of the governing IA documentation as well as some of the organizations either directly or

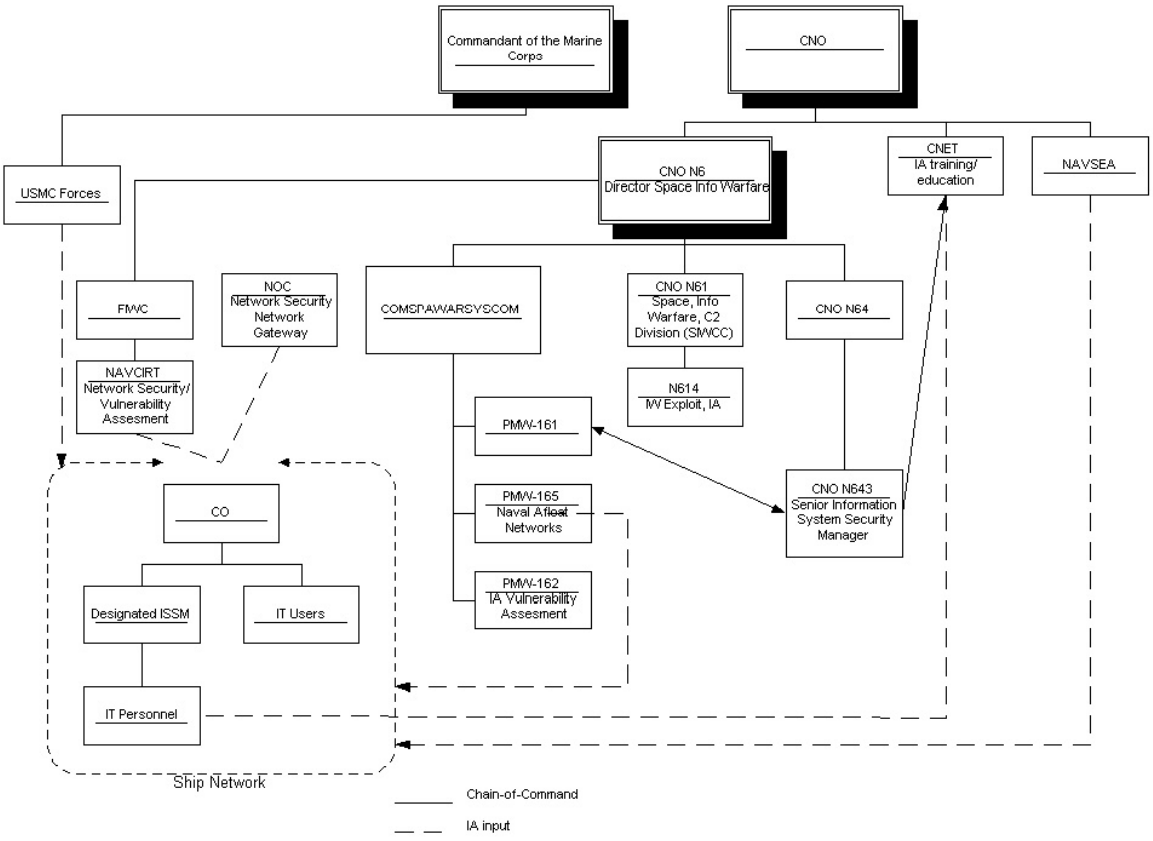

Figure 2-1. DoN IA Organization Chart.

indirectly involved with IA, the sought after "defense-in-depth" strategy appears to be little more than defense (of objectives) by compartmentalization. It is also apparent that considerable gaps and significant overlaps abound in the current IA program. Though repetitiveness and fragmentation will continue to proliferate throughout the IA policy, the DoN could greatly enhance its IA efficiency, and sum up its IA objectives into an overall strategy, by simply adopting a common but robust IA management tool that synchronizes the entire DoN IA organization.

B. INTRODUCTION TO INFORMATION ASSURANCE RISK MANAGEMENT

LCDR Ernest Hernandez developed IARM as a Masters level thesis at the Naval Postgraduate School. Like its cousin ORM, from which it was derived, IARM applies common principles and syntax to IA, facilitating greater standardization and a more vigorous defense. In addition, ORM has been credited with "dramatic results" since its inception into the DoN (OPNAVINST 3500.39A), which suggest that the adoption of IARM could also provide a similar outcome (Hernandez p. 61).

IARM is intended to be a simple yet hearty language that allows each person familiar with IARM to speak about IA in a common syntax. While there are still, and will continue to be, overlaps and gaps in the numerous DoN organizations that deal with IA, IARM would greatly enhance the inter-workings of these organizations with each other and the warfighters in the fleet. Through the employment of IARM, those involved with IA would finally be able to clearly understand each other (Hernandez p. 50).

C. PRINCIPLES

IARM is based on four principles that must be present throughout all aspects of the IARM process. These principles facilitate constructing and managing an effective risk management plan.

1. Accept No Unnecessary Risk

Risk assessment is a process of understanding how the corruption, loss, or theft of information resources will affect one's critical infrastructures. Risk assessment is not an exact science, and consequently it is a very difficult task (Denning 386). New vulnerabilities and exploits are constantly being discovered, and it is almost impossible to

determine the likelihood of attack on one's systems. Information values are also somewhat ambiguous, but can at least be placed in the categories of replacement costs, unavailability costs, and disclosure costs (Denning 387). Overall, risk is inherent to information systems as it is almost impossible to predict every vulnerability and consequence.

Although risk assessment is difficult, risk management is a deliberate process of identifying and understanding likely risks and subsequently deciding upon and implementing actions to reduce risk to a defined level. It is here in the risk management phase that the first principle must constantly be applied. If a risk or new vulnerability is identified, then an appropriate countermeasure must be installed. If new hardware is installed, it must comply with current security measures. Even if all risks/vulnerabilities cannot be discovered and addressed, accepting no unnecessary risks in mission critical requirements can certainly mitigate them.

2. Make Risk Decisions at the Appropriate Level

Making risk decisions at the appropriate level is the second and perhaps the most important principle of IARM. LCDR Hernandez suggests, "the appropriate level for risk decision is the one that can allocate the resources to reduce the risk or eliminate the threat and implement controls" (48). This statement appears to be a generality of leadership, as the leader is solely responsible for the assigned information resources.

Though one leader is ultimately responsible, numerous people are involved in this process. The person who controls allocation of resources may not understand the controls needed to reduce the threat, and, conversely, the person who understands the threats may be asking for more controls than the available resources permit. Hence, the

leader must be able to mitigate these problems and must, therefore, have an understanding of both the available resources and control measures. It is here that the utility of IARM and the necessity of teaching to both the technician and the decision-maker become most evident. (Recall the distinction between IA "users" and "technical supporters.")

3. Accept Risk When Benefits Outweigh the Costs

The third principle of IARM is also clearly a responsibility of leadership, and the IA "user" vice "technical supporter." Even if accepting any risk is contrary to the IARM's first principle, a good leader understands the necessity for compromise and balance. Although vulnerabilities may be identified (by a technical supporter), an immediate countermeasure implementation may not be necessary if there is little chance of the vulnerability actually being exploited (as decided by a user). However, if a good leader does not understand the risks and controls, he is not able to make the necessary compromise. Thus, this principle, too, highlights the need for IARM training not only at the decision-maker level, but also emphasizes the need for the technician to be able to clearly describe the importance of the vulnerability and or countermeasure in terms the decision maker can understand.

4. Anticipate and Manage Risk by Planning

While not all risks can be identified in the beginning, managing those risks that are anticipated is much easier than attempting damage control. Correctly anticipating risks or problems in the planning stage allows for specifically-designed controls to be implemented from the start and facilitates maintenance and scalability of future controls needed for those unanticipated risks.

Not all risks are initially identifiable; however, implemented controls for future vulnerabilities must be interoperable with the original plan. Even if future controls address new perceived risks, the hodgepodge of controls may cause additional problems. Once a risk management plan is conceived, those risks and possible controls must be viewed and implemented in accordance with the plan's guidance.

D. BENEFITS

LCDR Hernandez identified numerous benefits of IARM. From these derived benefits, two things become clear: 1) IARM standardizes the IA the process for all persons involved, and 2) IARM provides a common syntax for those involved, which consequently derives a better way to do business. In addition to all of the benefits identified by LCDR Hernandez, IARM also addresses either directly or indirectly all of the objectives set forth by the DoN IA program, as illustrated in Table 2-1. (Chapter 3 of this thesis will assist IARM in addressing the "standardized IA training" DoN IA objective.)

1. Manages Information Assurance Risks

"[IARM] improves network and information assurance awareness among users, IT support personnel, and decision makers" (Hernandez p. 58). IARM would improve network and information assurance awareness among IT support personnel by providing a common syntax for them to discuss and address IA issues. In addition, by being a simplistic language able to be understood by all persons even remotely involved, IARM allows the user, technician, and decision maker to better understand IA and each other.

IARM	vs.	**Traditional Approach**
Systematic		Random, Individual-Dependent
System View		Point Solutions
Proactive		Reactive
Integrates All Types of Threats and Vulnerabilities Into Planning		Security as After-thought Once Computer Network Services are Initiated.
Common Process/Terms of Information Assurance		Non-standard
Conscious Decision Based on Risk vs. Benefit		"Can Do" Regardless of Risk

Table 2-2. "IARM vs Traditional Approach" (From: Hernandez p. 51).

By simply understanding the Risk Assessment Code, the Probability of Occurrence, and the Severity Category, IARM can help even the least knowledgeable understand the situation.

IARM is an enabler to "adopt a risk-based life cycle management approach in applying basic minimum uniform standards for the protection of DoN information technology resources that produce, process, store, or transmit information" (CNO N643 p. 2-3). This objective is directly answered by the very definition of IARM—"the process of dealing with risk to information and data that is inherently associated with information operations and information systems, which includes risk assessment, risk decision-making, and implementation of effective risk controls" (Hernandez p. 37).

2. Increases the Level of Information Assurance

"Discussing issues of security can raise the general level of interest and concern" (Hernandez p. 58). IARM does help IT personnel raise the level of security by identifying potential problems and the best controls to implement in correcting them.

Because IARM provides a common language that all involved can understand, general security levels will increase as one and all become more security-knowledgeable.

In addition, IARM can "protect the confidentiality, integrity, availability, authenticity, and non-repudiation of information and resources to the degree commensurate with their value, as determined by the required level of IA, classification or sensitivity level and the consequences of their exploitation or loss for a period required by the mission supported" (CNO N643 p. 2-3). As the principles of IARM become more commonplace, classifications, sensitivities, and consequences of IA will also increase. A common IA syntax will increase security knowledge, which in turn will raise security conscientiousness.

3. Identifies Information Assurance Assets, Procedures, and Risks

IARM assists in providing "a comprehensive list of assets and vulnerabilities associated with those assets" (Hernandez p. 58). By using the IARM principles, potential vulnerabilities and controls can be easily identified. However, more than just cataloging assets, the list itself becomes part of the IARM plan. Proper documentation of these vulnerabilities and controls can assist not only in identifying current assets, but also in illuminating the need for interoperability issues of future assets.

Using IARM principles, one can easily "conduct an assessment of threats, identify the appropriate combination of safeguards from the IA disciplines, and apply an appropriate Certification and Accreditation (C&A) process for each specific information system developed by a program office and for each local site employing networks and deployed information systems" (CNO N643 p. 2-3). IARM by its very definition is risk management for IA. The employment of IARM and its principles will not only assess

threats and identify safeguards, but will also improve the C&A process by allowing all persons involved with IA to finally speak with a common understanding.

4. Provides Cost-effectiveness and Efficiency

"Decision makers now have an improved basis for implementing controls, justifying expensive or inconvenient controls, and continuing the search for more effective controls should the need arise" (Hernandez p. 58). It is often difficult to justify expensive controls. IARM alleviates this problem by allowing the technician, who identifies the vulnerability and understands the needed control, to communicate effectively with the decision maker, who ultimately holds the "purse strings." Allowing these two entities the ability to communicate will not only facilitate the decision maker's ability to make a better decision, but will also guide the technician's efforts and understanding of the larger issues.

IARM facilitates the employment of "…efficient procedures and cost-effective, information-based security features on all Information Technology (IT) resources procured, developed, operated, maintained, or managed by DoN organizational elements to protect the information on those resources" (CNO N643 p. 2-3). With the proper understanding and documentation of IA assets via IARM as previously discussed, more efficient and cost-effective IA procedures can be derived. In addition, although these plans and procedures may vary based on different organizational assets and requirements, IARM facilitates a common understanding of IA necessities and interpretabilities DoN-wide, thereby increasing efficiency, lowering costs, and improving security.

5. Standardizes Information Assurance Training

"Finally, IARM is a continuous, non-static process that can be applied by users, IT support personnel, and decision makers alike, giving the whole chain of command the opportunity to personally make a positive contribution…" (Hernandez p. 58). This perhaps is the greatest benefit IARM has to offer. From the decision maker to the technician, IARM allows the entire chain of command to communicate and contribute to IA.

By being a standardized process itself, IARM will both necessitate and facilitate the establishment of "… standardized IA training within the DoN" (CNO N643 p. 2-3). Not only will IARM permit the entire chain of command the ability to contribute to IA, but standardized IARM training Navy-wide allows the entire DoN to contribute and raise the level of IA. It is this objective that facilitates the necessity for this thesis and follow-on work in designing DoN IARM training.

E. SUMMARY

The current DoN IA policy and organizational structure is confusing and riddled with numerous gaps and overlaps. Realizing the Navy's IA problem, LCDR Hernandez developed IARM as an answer to the lack of an overall IA strategy. By adopting the simple principles of IARM, the Navy can not only improve upon its traditional method of dealing with IA, but also greatly improve it. The simplicity and numerous benefits of IARM certainly make it an attractive solution for the DoN's IA problem.

III. TRAINING

A. DEVELOPING A COURSE—TRAINING PROJECT PLAN (TPP)

The Chief of Naval Education and Training (CNET) is responsible for the training of all Navy personnel. CNET Instruction (CNETINST) 1550.10B provides policy and defines the responsibilities for "the production, approval, implementation and cancellation of training programs and materials." It also provides policy for the production of training material using two approved CNET instructional systems design/development (ISD) methods—Naval Education and Training (NAVEDTRA) manual 130 and NAVEDTRA 131. (ISD is a systematic design for training that focuses on specific objectives.)

NAVEDTRA 130 is a "task-based" curriculum management manual that focuses on a specific job to be accomplished by the student after the training is complete. By focusing on the job and the skills or tasks necessary to perform the job, a task-tailored curriculum can be developed. In contrast, NAVEDTRA 131 is a "personnel performance profile (PPP) –based" manual that focuses on background knowledge, the performance of tasks/functions, and the operations and maintenance of hardware (equipment/subsystems/systems). By careful analysis of the factors involved, this method produces a performance outline on which to base the curriculum.

To determine which of these methods and manuals is best suited for the development of IARM training, the goal of IARM training must be determined. IARM is designed to be an aid in managing IA risks and to be a common syntax for all of those involved with IA. Though IARM certainly has the ability to aid in different jobs, simply "performing" IARM will not accomplish any specific tasks—ruling out the task-based

method. Undoubtedly, the goal of IARM training is to impart the background knowledge of applying the IARM principles to numerous tasks, which clearly falls under the PPP method. By learning IARM and its principles, the student is able to apply IARM in whatever manner necessitated by the student in any particular situation.

Figure 3.1 illustrates the entire course development process for the PPP process. Although it is necessary to complete all of these stages to fully develop and implement a new course as set forth by the Naval Education and Training Command (NETC), all stages are not necessary to justify initial course development.

The "planning stage" will be the main focus of this section, as it contains the "Training Project Plan" (TPP), which contains requisite information for course development. However, like the PPP process as a whole, some of the requirements for developing a TPP are necessary strictly for NETC administrative purposes. Though these requirements—establishing a Course Identification Number (CIN), Course Data Processing Code (CDP), initiating entries for the Catalog of Navy Training courses (CANTRAC) and the Navy Integrated Resources and Administration System (NITRAS)—are necessary for a complete TPP, they do not impact the scope of course development for this thesis (NAVEDTRA p. 2-1-1). By simply examining portions of the TPP, enough material becomes apparent for further development of an IARM course.

The TPP contains basic preliminary information about the course including the intent and scope of the curriculum, as well as the Fleet-need, which generated the initial requirement for the curriculum. When finally approved, the TPP becomes the authorization to undertake the development of a new course. (CNET approves TPPs for

PLANNING → ***CCA/Functional Commander/CNET/OPNAV***
- Training Project Plan (**TPP**)

STAGE ONE
- PPP Table List
- New and Modified PPP Tables
- Training Path System (**TPS**)

STAGE TWO → ***CCA***
- Preliminary Training Course Control Document (**TCCD**)

STAGE THREE
- Instructional Materials Cross Section (If Required)
- Lesson Plan
- Trainee Guide
- Tests
- Other Support Materials

STAGE FOUR → ***CCA***
- Course Pilot
- Pilot Course Monitoring Report

STAGE FIVE
- Final Curriculum
- Final **TCCD**
- Letter of Promulgation

EVALUATION
- Internal
- External [→ = ***Approval Authority***]

Figure 3-1. Curriculum Development Process (From: NAVEDTRA 131A p.1-5).

new courses unless the resource requirement is beyond CNET, upon which CNET forwards the TPP to the appropriate CNO sponsor (CNETINST p. 4)).

1. Justification for Course Development

The first step in developing a TPP is to identify the reason or need for the new course. NAVEDTRA 131A lists several acceptable course justifications: (1) Navy Training Plans (NTPs), (2) tasking by higher authority, (3) internal course reviews and local command initiatives, (4) external feedback, (5) surveillance, and (6) training appraisal (p. 2-2-1). Justifications for implementing IARM in the DoN were presented in LCDR Hernadez's thesis and Chapter Two of this thesis and are further represented by Figures 3.2, which illustrates current DoN Network Operations, and 3.3, which illustrates the future of DoN Network Operations. While a strong case has been

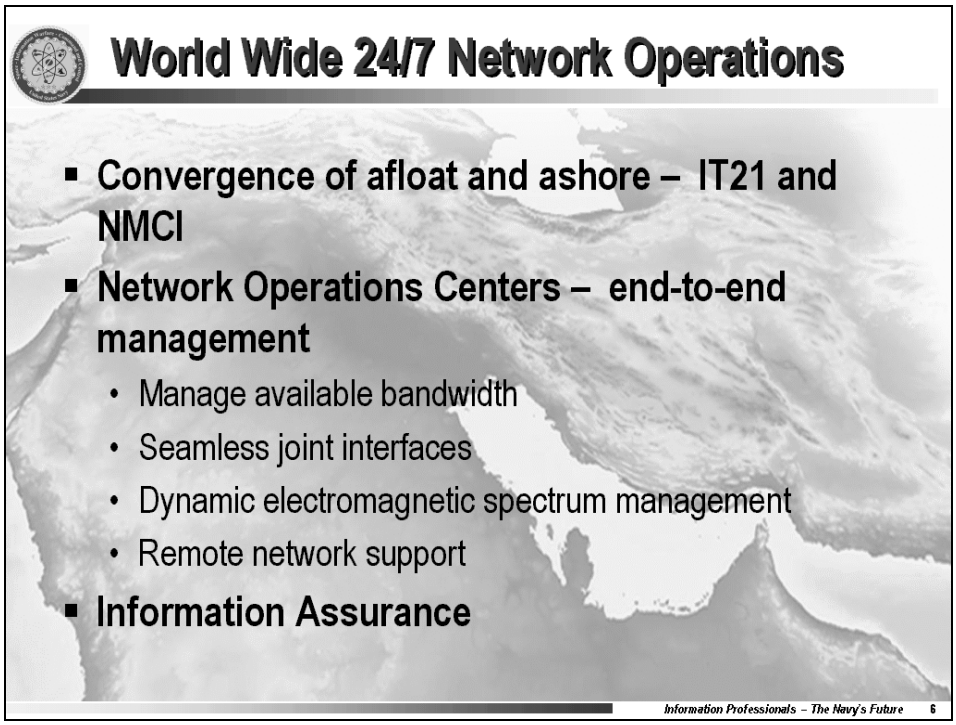

Figure 3-2. Current DoN Network Concerns. (From: VADM Mayo Information Professionals presentation).

made for exploiting IARM, does it meet the established criteria and warrant justification for development of an IARM course?

The necessities for IARM training do in fact meet a number of the NAVEDTRA conditions. The CNO and N643 have both established the need for IA and standardized IA training (See Table 2-1), thus establishing tasking from the highest authority in the DoN. In addition, by observing two DoN organizations and the DoN-governing IA publication (See Chapter 2), it becomes apparent that a standardized IA syntax is needed to integrate all of the current IA organizations and assets, thereby also meeting the surveillance criteria as well. (Although it is not necessary to meet all of the NAVEDTRA course-requirement criteria, implementation of a pilot IARM program would not only

prove IARM's usefulness, but also serve to establish and meet additional NAVEDTRA criteria (See Chapter 4, Recommendations).)

2. Impact Statement

An impact statement is also required to further justify the necessity of the course by highlighting the negative impact of not developing it. Though numerous benefits of IARM and their potential impacts on the DoN have already been discussed clearly showing the need for IARM, it is difficult to derive a negative impact statement. However, as corroborated by Figures 3.3 and 2.1, Network Operations and, consequently, IA will continue to permeate all aspects of the DoN; therefore, by not developing an IARM course, the DoN is destined to keep performing IA in the same inadequate way it currently employs while its network-centric operations continue to expand.

3. Mission Statement

The mission statement for an IARM course is dependent on its student population. For example, the mission of IARM taught to decision makers and senior personnel may be to increase the understanding of IA through IARM in order to be able to make better-informed IA-related decisions. For the technical expert, IARM's mission may be to raise IA understanding in order to assist in protecting IA resources, to develop a comprehensive IA system, and to facilitate standardized IA communications within the DoN. Because IARM would assist different personnel in a variety of ways, it becomes necessary to examine those who need to know and for what purpose before a tailored mission statement can be derived.

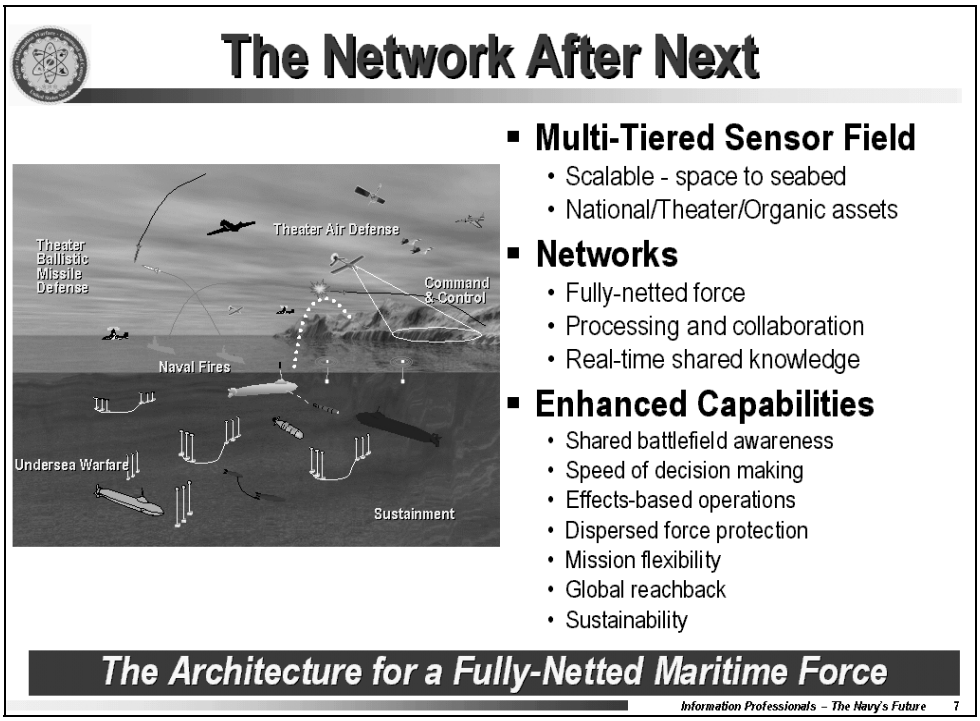

Figure 3-3. "The Network After Next" (From: VADM Mayo Information Professionals presentation).

4. Further Requirements

There are additional requirements for the TPP that will not be discussed. Like the administrative details referenced earlier, the additional requirements are either administrative in nature, course specific, or not applicable to this level of course development (i.e., "Course Data Page," " Resource Requirements," and "Safety Risks and Hazardous Materials Exposure") (NAVEDTRA p. 2-7-1). A requirement, impact statement, and mission statement are sufficient for the planning stages of an IARM course. In order to progress into Stage 1 and further areas of course development, the appropriate level of the course and to whom it should be taught must be answered next.

B. LEVELS OF INSTRUCTION

It is important to emphasize that a distinction exists between training and education. As previously discussed, the current DoN IA policy demonstrates an apparent difference between "users" and "technical supporters." In fact IARM, too recognizes this dissimilarity, yet through its use of a standardized syntax, significantly diminishes the divergence. However, because the separation does exist, it is important to briefly spotlight the related disparity between the two.

1. Training

Both IA users and supporters must be given instruction in IARM to understand and use it, but the degree of understanding and therefore the level of instruction becomes one of the distinguishing arguments between users and supporters. Webster's Dictionary defines "train" as "…to form by instruction, discipline, or drill" (p. 1252). In other words, the act of training is simply to teach by instruction or repetitive performance ("drill") in order to perform a task. In the case of IA users, they need only be proficient in the syntax of IARM in order to be qualified to perform their IA role. In contrast, the technical supporter shoulders a greater IA burden and needs, therefore, to be an IARM expert.

2. Education

On the other hand, Webster's Dictionary defines "educate" as "…to train by *formal* instruction and *supervised* practice especially in a skill, trade, or profession" (p. 367) [emphasis added]. IARM "training" is sufficient for a user to be able to understand the basic IARM syntax and to perform his decision-making role, however technical supporters need more. The IA technical supporter, who has a much greater role in IA, must understand all aspects of IARM to utilize it to its fullest potential and would

consequently benefit more from "formal" training and "supervised" practice. In addition, the technical supporter needs IARM to perform a designated "…skill, trade or profession," which implies a higher degree of IARM knowledge and education vice training.

3. Semantics

Though semantically this difference may seem trivial, it greatly impacts the DoN organizational structure. Comprised of officers versus enlisted, managers versus specialists, primary versus secondary versus collateral duties, and communities and rates versus assigned billets, the DoN rank and job structure only further emphasize the distinction between user and technical supporter and between education and training.

C. WHO NEEDS TO KNOW

Thus far, it has been demonstrated that not only is an IARM course necessary, but there is enough basic information to meet NETC criteria for a new course. But it has also been shown that a controversy as to the type and/or level of the education/training for the proposed IARM course also exists due to the organizational structure of the Navy. It is then the goal of this section to further examine this controversy and determine exactly who needs to know what.

The Navy has numerous "standards," such as Naval and Occupational Standards (OCCSTD), Naval Enlisted Classification (NEC) descriptions, and Navy Officer Billet Classification (NOBC) that list applicable skills and knowledge for Navy personnel. By a closer examination of Navy standards, limited here to the complement of a cruiser-size ship, a good understanding of requisite IARM knowledge can be derived. (It is important

to note that this is the first step in developing a Personnel Performance Profile (PPP). See Figure 3-1.)

1. Officers

The Navy Officer Occupational Classification System (NOOCS) is "…the method the Navy uses to identify skills, education, training, experience and capabilities related to both officer personnel and manpower requirements" (NAVPERS 158391 p. 3). The system is comprised of code structures that form the basis for "… officer manpower management and officer personnel procurement, training, promotion, distribution, career development and mobilization" (p. 3). The code structure is further broken down into four subsystems—Designator/Grade, Subspecialty (SSP), Navy Officer Billet Classifications (NOBC), and Additional Qualification Designation (AQD)—which help to further specialize and categorize Naval Officers.

Although the NOOCS is used to classify an officer, an examination of all of the classifications of officers in the DoN is not only unnecessary, but also impractical. For example, the "designator" sub-classification can be subdivided yet further into the following: unrestricted line officers (URL) (officers of the line who are not restricted in the performance of duty), restricted line officers (officers of the line who are restricted in the performance of duty by having been further designated for special duties), staff corps officers (officers belonging to one of the eight staff corps (e.g., medical, dental, chaplain, etc.)), limited duty officers (officers of the line appointed in broad occupational fields indicated by their former warrant designator or enlisted rating), chief warrant officers (officers of the line appointed to chief warrant officer for the performance of duty in technical fields indicated by former enlisted ratings group), and a few others (NAVPERS

158391 p. A-2). Clearly not all of these designators would need the same level of IARM training (e.g., Chaplains have less involvement with a LAN whereas IT warrant officers have been commissioned because of and are limited to their specialty within the Information Technology rating). But then how is the requisite level of knowledge, or in this case IARM training, determined for an individual officer?

a. The Designator/Grade

The Designator/Grade structure of the NOOCS consists "…of designators and grades that provide a framework for officer career development and promotion" (NAVPERS 158391 p. 3). This sub-classification is the primary administrative means for "… classifying, identifying and documenting officer manpower resources and requirements" on a very large scale. The "designator" structure identifies, among other things, "…primary specialty qualifications" of officer groups as a whole and would therefore differentiate, for example, between an Information Professional Officer (1600) (see Information Professional) and a Surface Warfare Officer (1110). Though the designator can be used to determine IARM requirements on a very broad scale, as previously discussed, it does little to impact individual officer requirements within a particular designator.

The "grade" structure identifies "…occupational levels associated with the scale of naval officer paygrade and rank" (NAVPERS 158391 p. 3). Like "designator," "grade" alone cannot directly determine the IT involvement of a single officer, but does factor into the eligibility and determination of the billet the officer can be assigned.

Billets are primary jobs within a designator determined by rank and eligibility. Within a designator, officers are assigned billets (e.g., engineer,

communications officer, deck officer, etc.) in addition to their primary designator duties. While billets can show the need for specialized training, they cannot be the sole determining factor.

b. The Navy Officer Billet Classification (NOBC)

The NOBC structure functionally identifies "…officer billet requirements and officer occupational experience acquired through billet experience or through a combination of education and experience" (NAVPERS 158391 p. C-3). Although billets alone cannot determine required training, the NOBC recognizes the specialty training that an officer does get by having filled certain billets. Perhaps by identifying those NOBCs associated with IA, the Navy could implement IARM training at those billet-specific schools, as well as the designator school itself.

c. Sub-specialty Codes

The Subspecialty (SSP) structure "…identifies postgraduate education (or equivalent training and/or experience) in various fields and disciplines" (NAVPERS 158391 p. 3). Though the designator is the primary code used to specify the area of specialization (or specialty), certain billets within the designator may require additional qualifications beyond those indicated by the designator code alone, hence the need for a subspecialty code (NAVPERS 158391 p. B-2). Although subspecialty codes illustrate the need for additional qualifications beyond those of just the designator, subspecialty codes are grouped by training category, not by designator.

d. The Additional Qualification Designation (AQD)

The AQD structure identifies "…additional qualifications, skills and knowledge required the duties and/or functions of a billet beyond those implicit in the billet, designator, grade, NOBC, or subspecialty…" (NAVPERS 158391 p. D-1). The

AQD are those qualifications within the designator that ensure junior officers receive the proper training and skills required to become a senior officer in the designator.

e. Illustration of NOOCS In a URL Junior Officer

As stated previously, by limiting discussion of the requisite for IARM training to a small sample group, the results can be applied to the officer classification system as a whole. Within the limits of a ship's complement, this discussion will focus on the URL Surface Warfare Officer (SWO) designator. The SWO is primarily concerned with all aspects of ship handling and tactical employment of the ship with the rank structure (Ensign to Admiral) designating levels of responsibility within the designator (i.e., Ensigns through Lieutenants are usually focused on ship handling, Lieutenants through Commanders are usually focused on tactical employment of the ship, Commanders and Captains are concerned with overall responsibility of the ship, and Captains and above are concerned with employment and readiness of groups or fleets of ships). Once designated a SWO, an officer progresses through the stages of the designator as his rank and experience increase, ultimately producing a well-rounded officer with all of the requisite surface warfare knowledge. Can the NOOCs also aid in determining and tracking the requisite for IARM training for a SWO?

Upon initial designation as a SWO (designator 1110), an officer goes to a community-specific school (in this case Surface Warfare Officer School (SWOS)) where he learns the fundamentals for his designator for his specific rank, regardless of his future assigned billet. During the course of a SWO's career, he returns to SWOS for each different fundamental level (Division Officer/ship handling, Department Head/tactical employment, XO, and CO/over-all ship responsibility). If IARM is designated as a

"fundamental" for the SWO designator, does it not make sense then to incorporate IARM training at SWOS itself?

After SWOS, a SWO is assigned to a ship and a certain billet. For example, a SWO assigned to the communications officer (COMMO) billet is a fairly low-grade officer directly responsible for, among other things, the ship's LAN. IARM would be important to the COMMO in facilitating his billet-specific responsibilities of IA technical support for the entire ship. Therefore, because the COMMO billet has a specific need for IARM, IARM could also be taught in those billet-specific schools that demonstrate a requirement for IARM.

However, the COMMO is directly answerable to a mid-grade officer assigned as the operations officer (OPS), who in turn is answerable to the senior officers, executive officer (XO), and commanding officer (CO), the lattermost of whom is ultimately responsible for the ship and everything on it. If the COMMO were the only officer familiar with IARM because it was only taught to specific billets, he would not be able to effectively communicate his IA needs to his chain-of-command (superior IA decision makers). Although members of the chain-of-command may have been a COMMO as a junior officer and may have had IARM knowledge, having held a specific billet is not necessary to advance within the designator. Therefore, IARM knowledge is a requisite for more than just the COMMO billet, as the ship's entire chain-of-command may become involved in an IA decision regardless of their present or past billets.

A SWO earns an AQD upon completion of a major milestone (such as qualifying as Officer of the Deck) within the designator. If IARM were deemed to be necessary for an entire designator, yet not taught in SWOS, then making an IARM AQD

for those officers having had IARM training or obtaining an IARM qualification would also aid in ensuring only qualified officers handled IA. In addition, making an IARM AQD a requirement for advancement within the designator would ensure familiarization of every level of the chain-of-command with IARM.

Lastly, requiring officers/billets to have a subspecialty code would also ensure those who needed IARM training would have it. Information Systems and Operations is a curriculum offered by the Naval Postgraduate School (NPS) that fulfills the requirements for obtaining a computer technology subspecialty code. This interdisciplinary program provides students with the knowledge of information systems technology so that the student may gain proficiency in "…information operations, economics and management necessary for the critical warfighting-decisions needed in Information Age conflicts" (NPS Catalog p. 41). The simple addition of IARM to this curriculum would not only help achieve the curriculum's goals, but would also be a useful tool that the SWO could use upon his return to the Fleet.

f. Senior Decision Makers

Though discussion up to this point has been about Surface Warfare Officers in general, it has been more targeted at junior officers. Can IARM be taught to senior-level officers as well? (See Appendix C. Section E.)

The Naval Postgraduate School hosts the "Center for Executive Education." Intended for "senior DoN/DoD [Department of Defense] executives," its mission is to promote better understanding of "emerging strategic and policy issues and practices…" ("About the CEE"). As part of its strategic direction, the CEE intends to provide: 1) "…an environment where defense issues may be better defined and

understood," and 2) "…executive education … that furnish the *tools* and skills necessary to add value to senior defense leader" ("About the CEE") [emphasis added].

Not only would IARM be an applicable addition to this program, but it would also greatly enhance two of the courses presently being offered. "Leading Change in the Information Age" focuses on increasing the "…*problem solving* ability in information superiority of senior defense executives in performing their demanding leadership roles" ("Other Programs") [emphasis added]. One of the primary focuses of this course is to familiarize the executive with "…the underlying principles of technologies and on the *ability to analyze and synthesize effective and flexible strategies*" ("Other Programs") [emphasis added]. The other course, "Chief Information Officer" is designed "…to better prepare military and civilian managers within the Department of Defense to manage the complexity of information technologies" ("Other Programs"). Not only would the CEE be an effective way to teach IARM to Senior Decision Makers, but the CEE would also have to do very few modifications to its existing courses in order to incorporate IARM.

g. Information Professionals

Though not currently a part of a standard ship's complement, the new Information Professional (IP) community still bears investigation. (See Appendix C. Section C. The IP community did not exist at the time of LCDR Hernandez's thesis, hence the "Information Technology Support Corps" title.) Brought into being because of the realization that more than a technical infrastructure was needed for a Network-centric Navy, the IP community is intended be a cadre of operationally-savvy information professional officers providing a direct link between the warfighter and the technical

supporter. The mission of the IP community is to "…provide expertise in information, command and control, and space systems through the planning, acquisition, *operation, maintenance and security* of systems that support Navy operational and business processes" (Mayo to NAVADMIN) [emphasis added]. Defined properly, shipboard IT infrastructure support assigned to IPs, which includes elements and responsibilities of Combat Information Center Officer (CICO), Communications Officer (COMMO), Electronic Maintenance Officer (EMO), and Combat Systems Officer (CSO), is based on a job to be done rather than a responsibility of a billet. The IP is intended to come from the "traditional" warfare communities (in the scope of this discussion, Surface Warfare) and to help the warfighter via his past "operational experience" and competency in "…network and computer system technologies," "…computer and network security/*information assurance* [emphasis added]," " information management," and "information technology architecture" (Mayo to NAVADMIN). See Figure 3-3. The establishment of the IP community, and hence the new link between decision maker and supporter, will greatly enhance not only the Navy's network-centric capabilities, but also its IA.

Undoubtedly the IP will prove to be a professional link between the decision-makers and technical supporters but is this not also the proposed role of IARM? Similar in tasking, IARM is anticipated to be a link through the use of common syntax, whereas IPs are intended to provide a link by means of their experience and knowledge. However, by combining the experience and knowledge of the IP with the common syntax of IARM, the IP has a better way to communicate with both the decision maker and technical supporter, thereby fostering a stronger relationship between all three.

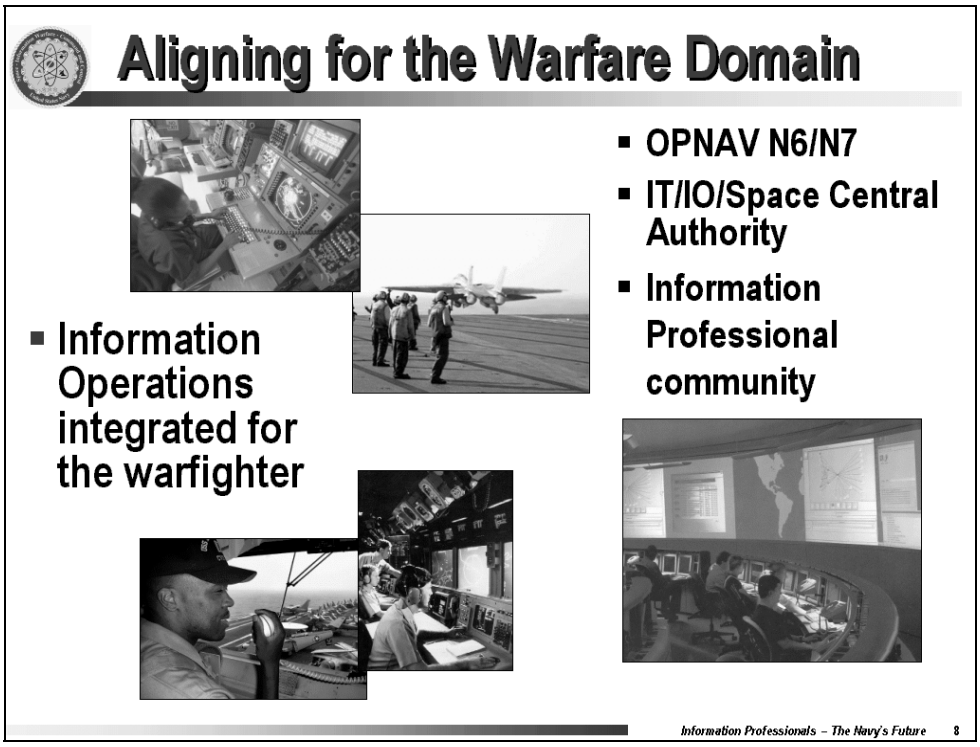

Figure 3-4. "Aligning for the Warfare Domain" (From: VADM Mayo Information Professionals presentation).

Even though IARM would enhance the IP community it is important to note that the decision maker/technical supporter ratio in the Fleet is far greater than the number of IPs in the community. However, in lieu of an IP, IARM alone can still bond the decision maker and technical supporter as long as they both have knowledge of IARM.

2. Enlisted Personnel

Like the NOOCS used for Officers, the Navy Enlisted Occupational Classification System (NEOCS), consisting of the enlisted rating structure and the Naval Enlisted Code (NEC) structure, serves to categorize the enlisted sailor (NAVPERS 18068F p. 1). The enlisted rating structure consists of "…occupational fields (i.e., broad groupings of similar occupations), ratings (i.e., occupational specialties) and rates (i.e., a paygrade

within a rating)," which provide a "…framework for enlisted career development and advancement, and is the primary administrative means for classifying and identifying enlisted personnel" (p. 1).

Though the Officer and Enlisted Occupational Systems appear similar and perform basically the same function, the Enlisted system is more explicit in its categorization. For example, Occupational Standards (OCCSTDs) "…express the Navy's minimum requirements for enlisted occupational skills," but do so by stating exactly "…what enlisted personnel must do in their rate or rating" (NAVPERS 18068F p. 5). By plainly cataloging the tasks for each rate and rating, specific knowledge required to perform the task may be derived. (This task-based method of determining required knowledge falls under the guidance of NAVEDTRA 130A, providing yet another formal way to look at implementing IARM Navy-wide.)

On the other hand, the Navy Enlisted Classification (NEC) structure supplements the enlisted rating structure "…by identifying a non-rating-wide skill/knowledge/aptitude/qualification that must be documented to identify both people and billets for management purposes" (NAVPERS 18068F p. 3). The enlisted NEC is similar to the Officer's NOBC or subspecialty code in that it is more skill-specific rather rate-specific. Although NECs are skill-specific, they still tend to apply only to those ratings that would need that particular skill.

a. Applicable Rates

Because the OCCSTDs list specific groupings and tasks assigned each rate and rating, it is much easier to specify which enlisted personnel would most benefit from IARM training. In addition, the NEC structure also narrows down specific rates

associated with specific skills. Utilizing these two main categories, it is fairly easy to indicate which enlisted rates would most benefit from IARM.

To determine which rates would best benefit from IARM, skills are examined first. Defense grouping NECs "…identify individuals in paygrades E1-E3 that have received training, are in training, or have an aptitude for training in one of the general Occupational Areas" (NAVPERS 18068F p. 3). Under this category, two occupational areas might seem to deal with IA related issues: DG-9710 Electronic Equipment Repairman and DG-9720 Communications and Intelligence Specialist. (Though some may argue that other categories are applicable, these categories were chosen based on the fact that they were the only ones that dealt specifically with "Communications" and "Electronics.") These areas contain the following rates:

ST (Sonar Technician)
TM (Torpedoman's Mate)
FT (Fire Control Technician)
MT (Missile Technicians)
ET (Electronics Technician)
AT (Aviation Electronics Technician)
CTM (Cryptologic Technician (Maintenance))
FC (Fire Controlman)
OS (Operation Specialist)
SM (Signalman)
IT (Information Technician)
IS (Information Specialist)
AC (Naval Aircrewman)
AW (Aviation Warfare Systems Operators)
EW (Electronics Warfare Technician)
CTI (Cryptologic Technician (Interpretive))
CTO (Cryptologic Technician (Communications)
CTR (Cryptologic Technician (Collection)
CTT (Cryptologic Technician (Technical)) (NAVPERS 18068F p. 3).

After having narrowed down the Defense Grouping NECs, the Rating and Special Series are examined next. Rating NECs are applicable for a limited number of

ratings, whereas Special NECs apply to groups of ratings. However, these NECs are grouped by ratings themselves so to taper the focus only those ratings that were listed under the Defense Grouping NECs and are part of a standard ship's complement, are examined (ST, TM, FT, MT, ET, CTM, FC, OS, SM, IT, IS, EW, CTI, CTO, CTR, CTT). To narrow the criteria even more, the Occupational Fields and their associated ratings can be used.

Occupational fields are a part of the NEOCS system and are broad groupings of similar occupations used to "…organize the analysis, management, and administration of Navy ratings" (NAVPERS 18068F p. 2). By applying the Occupational Field categories with the ratings previously identified, broad occupations are derived. For example, the rates previously identified (ST, TM, FT, MT, ET, CTM, FC, OS, SM, IT, IS, EW, CTI, CTO, CTR, CTT) break down into occupational groupings of:

"General Seamanship" (SM, BM (Boatswain Mate)
"Ship Operations" (OS, QM (Quartermaster)
"Weapons Control" (ET (Electronics Technicain), FT, FC)
"Ordnance Systems" (GM (Gunner's Mate), MN (Mineman), MT, TM)
"Sensor Operations" (EW, SGG, STS (Sonar Tecnician (Submarine))
"Cryptology" (CTA, CTI, CTM, CTO, CTR, CTT)
"Communications" (IT), and
"Intelligence" (IS) (NAVPERS 18068F p. B-1).

Examining NECs and their applicable rates, and then cross-referencing those rates with occupational fields gives the following: 1) numerous ratings are involved with IA related areas, 2) these ratings fall under many different Occupational fields, which seem to have little to do with IA, 3) as more and more systems become net-reliant, additional Occupational fields, and hence additional ratings are going to need to learn IARM. Although the NECs, occupational fields, and rates themselves can be used to determine which enlisted personnel require IARM, they cannot be the solely relied upon

(e.g., ITs and CTs are both concerned with IARM for IT infrastructure support, vice OSs which are more concerned with IARM as users). Like the officer community, enlisted billets and positions must also be examined to more thoroughly narrow the requisite for IARM training.

b. Applicable Billets/Positions

Having determined the ratings that would most benefit from IARM training, it is now important to look at specific enlisted billets/positions that would also benefit. Similar to the officer community in that a certain designator or skill is required to fill a certain billet, the enlisted community also has similar standards.

The Catalog of Navy Training Courses (CANTRAC) maintained by CNET, lists all DoN schools and their equivalent qualifications. In order to fill some billets, or ratings for that matter, certain schools are required. (The CANTRAC lists not only rating specific A and C schools, but also NEC schools.) For example, by performing a simple search of the CANTRAC for "information assurance," the following two courses were returned—Information Systems Administrator and Cryptologic Technician O Class A.

Information Systems Administrator is an enlisted NEC school that prepares "…technical personnel to administer a networked system with focus on the following functional areas: 1) Configuration Management: Manage changes, additions, and deletions to network system configurations; 2) System Management: Administration of network services, maintaining user accounts, access rights, and directory services; 3) Performance Management: Maintain system reliability statistics, performance checking of system communications pathways, and optimization of system and application

performance" ("CANTRAC"). Prerequisites are paygrades E4-E5 and rates of CTA, CTM, CTO, CTR, CTT, ETS, FT, IT, or STS. In addition, "…candidates must have completed one tour of duty working in the Information Systems environment and have a basic understanding of computers, information assurance (security), operating software, applications and computer internals" ("CANTRAC").

Cryptologic Technician O Class A is an enlisted A school whose graduates "… possess the necessary skills in entry level networking, information assurance, and cryptologic communications equipment and systems to perform, with supervision, the duties of a communications operator at his initial field assignment" ("CANTRAC"). Because this is an A school, requirements are different than that of an NEC school and entail a certain ASVAB score, completion of the 10th grade or higher, possession of a SECRET security clearance, and be a SN (Seaman) or CTO.

The CANTRAC is useful in identifying any matching schools and their associated degrees, which are necessary to fill specific billets and positions. The CANTRAC is also useful in identifying which rates would benefit from IARM training by listing all applicable ratings for specific schools. (Note that the ratings identified by the "Systems Administrator" NEC in the CANTRAC fall within the group already identified in the NAVPERS 18068-67B.) Although the CANTRAC can be very useful in identifying requirements and schools for ratings, NECs, and specific job and billets, the EDVR actually lists the jobs and billets that enlisted personnel fill.

PERSONAL DATA - PRIVACY ACT OF 1974

ENL DIST & VERIFICATION REPORT 21829 04/29/98 PPSUIC/ZIP 21829 PAGE NO. 1 EPMAC-EDVR-1080

1. ACTIVITY: CG 72 VELLA GULF | 2. UIC: 21829 | 3. EFFECTIVE DATE OF RUN: 98 02 24 | 4. RELEV. PAYDAY: | 5. ACCOUNTING PERIOD ENDING: 98 03 24 | 6. RIN: 2 | 7. ATO: FNO | 8. MANNING CONTROL AUTHORITY: CINCLANTFLT | 9. MMCC: 60B0

A SPECIAL	B PTIO	C DEBIT	D LOV	E NAME	F SOCIAL SECURITY NUMBER	G SEX	H ACTUAL RATE	I EPM	J ASSGN RATE	K DAP	L DNEC1 DNEC2	M NEC1 NEC2	N DEP	O DOB	P ADSD YR MO DA	Q BR CL	R OPEX	S ACTIVE DUTY OBLIGATION YR MO DA EXT MOS & DTH	T ESEN YR MO DA	U PNO YR MO	V SECD OR SEDCD YR MO	W DATE RECEIVED YR MO DA	X DUTY STAT UN	Y DUTY STATUS EFFECTIVE DATE YR MO DA	Z EDA OR EOL YR MO	1 PO OR PL AUTHORITY	2 SEC	3 UIC TO/FROM	4 VERIFY REMARKS OR PO PPSUIC
SECTION 04									*	*	* *	* *	TOTAL PERSONNEL ON BOARD						*	*	*	*							SECTION 04
RATE NEC				NMP RULE	CUR BA 0498 / P-9 BA 0199		P-9 NMP 0199		TEMP DUTY 3XX		COB 0498	POB1 0598 / POB2 0698			POB3 0798	POB4 0898		POB5 0998 / POB6 1098	POB7 1198	POB8 1298	POB9 0199	N RQN 0199		P RQN 0199	A RQN 0199				
PERS OFFICE ACTION. VERIFY ALL ITEMS LISTED IN COL KEY 4. REFER EDVRMAN FOR COL KEY DESCRIPTION AND CORRECTIVE ACTION WHERE REQUIRED																													
NOTE: PERSONNEL APPEARING IN SECTIONS 1 2 OR 3 ARE IDENTIFIED IN SECTION 4 COLUMN 2 WITH SEC 1, SEC 2, OR SEC 3 AS APPROPRIATE																													
		B		MULHOLLAND A		F	BMC		BMC		0000	00009575	00		840321	11	16	990205			0009			PO		9809	B0498	1	20111	
		S		WILLETTS RIC		M	BMC		BMC		0000	01610164	S0		800818	11	35	981029		9810	8405	960930	PL	960930	9810	B0308	2	42056	
				CHARLES MELV		M	BM1		BM1		9595	***10000	A0		840619	11	26	980816	16	9912	9501	971205	100	971205			2		
		B		JONES JEFFRE		M	BM2	4	BM2		0000	01649545	B0		841103	11		000131		0211	9710	971110	100	971110					
				RACKLEY SHAR		F	BM2		BM2		0000	01600164	20	C10	850513	11		980725		9811	9310	960206	PL	960206	9811	B0708	2	42043	Z
		S		SMITH DENNIS		M	BM2		BM2		0000	0000	20		860623	11		020527		9811	9307	930712	PL	930712	9811	B0708	2	42043	Z
		S		SNYDER THOMA		M	BM2		BM2		0000	0107	10		861128	32	40	990210	990210	0002	9502	970209	100	970209			2		
				WEBER CRAIG		M	BM2		BN2		9595	***10000	20	B30	860821	11		020707		0011			PO		9811	B0498	1	20111	
				ALLEN CHARLE		M	BM3		BM3		0000	0000	A0		940111	32		021105	021105	0211	9405	971213	100	971213					
				ROVENSKI JAM		M	BMSN		BMSN		0000	0000	00		940420	11		980419		9901	9501	950120	PL	950120	9804	B2467	2		
BMC				90	1 1		1				1	1 1			1 1			2 1	1	1	1								
BM1				90	1 1		1				1	1 1			1 1			1 1	1	1	1								
BM2				90	4 4		4				4	4 4			4 4			4 4	3	3	3	1-							
BM3				90	5 5		4				1	1 1			1 1			1 1		1	1	3-			1				
BMSN				90							1																		
TOT					11 11		10				8	7 7			7 7			8 7	6	6	6	4-			1-				

Figure 3-5. Sample EDVR (From: Surface Warfare Officer Schools Command).

The Enlisted Distribution and Verification Report (EDVR) is a personnel management tool prepared monthly by the Enlisted Personnel Management Center (EPMAC). The EDVR facilitates making manning and assignment decisions by providing a detailed description of the personnel, billets, jobs and NECs required for a specific command. (The equivalent document for officers is the Officer Distribution Control Report (ODCR)). The same billeting data can then be used to illustrate training shortfalls and provide a common reference for communicating manning status between an activity and its Manning Control Authority (MCA) ("4-2 CG Resource Management.doc").

The EDVR is broken down into numerous sections that provide different statistical views of a command's manning. Sections 4 and 5 contain a statistical summary called the Navy Manning Plan (NMP) that designates the ship's "fair share" of current personnel assets available in the Navy (Surface Warfare Officer Schools Command). By using the EDVR and the NMP to determine a command's manning, required billets, and NECs, the billets that would most benefit from IARM as well as rates and the individuals themselves can then be determined.

c. Users and Supporters

Although OCCSTDs explicitly express enlisted occupational skills needed for a required rate, hence making it easier to determine who needs to know IARM, determining the appropriate level of training is still quite difficult. Like the officer community, enlisted personnel structures are designed to impart a common rating-specific knowledge to a sailor. By the time the sailor reaches a position of management within his rating, he must have a general understanding of all aspects of his rating.

Because a rating is a broad group of related information, simply identifying a rating that works with IA does not necessitate IARM training. Returning to the example of a ship's crew, recall that the COMMO is the officer responsible for the ship's LAN. Working for the COMMO are enlisted personnel of the IT rating.

Basic IT-knowledge, regardless of follow-on assignment, is taught at the IT-rating school ("A" school) at the beginning of an IT's career. "A" school teaches that information which is determined as being universally necessary for the rate. Specialized rating skills/knowledge required to perform a specific job or fill a specific billet are left up to focused courses (completion of which earns an NEC).

A very junior IT sailor (ITSN) needs to learn rate-basics before graduating to intermediate rate-knowledge. Therefore, even though the IT rating is responsible for the ship's LAN, the ITSN will initially be focused on the fundamentals of shipboard radio communication systems. A more senior IT (IT2), who already understands radio communications and may hold a LAN Administrator NEC, will be the one tasked specifically with LAN management.

Although there appears to be a clear break in requisite knowledge and rank of the IT, it is not always the case. In the preceding example, it was assumed that the IT2 held the LAN Management NEC. However, what if none of the IT personnel aboard held the required NEC? In this case, the ship would have to send one of its IT personnel to the required NEC course. IT2 probably would not be selected to go, as his knowledge of radio communications would still be of use to the ship's operations. On the other hand, ITSN would be the most likely candidate to receive the NEC, as he has little knowledge of the IT rating and therefore is of little immediate use to the ship; because he is new to the ship (assuming he has just reported from "A" school he will be aboard for almost 4 years), he will be able to fill the required NEC for the longest time.

Even though NEC appears to have a greater impact than rate in so far as who would benefit from IARM training, it cannot be relied on as the only basis for determination. A ship's EDVR may reflect that only one IT is required to have a LAN Management NEC; however, IA issues are not reserved for that person. Even if the EDVR has established the ship's requirement for a single LAN manager, the Navy has established that the entire IT rating is responsible for LAN management. In fact, the OCCSTD for the IT rating states "…Information Systems Technicians (IT) execute

information transfer with state-of-the-art multi-media technology such as fiber optics, digital microwave, and tactical and commercial satellites on a global basis; operate, manage and provide hardware and software support to multi-media Automated Information Systems (AIS) to include: mainframes, mini, and microcomputers, Local Area Networks (LAN's), Wide Area Networks (WAN's), and telecommunications; apply diagnostic and restoral techniques utilizing knowledge of electronic and operational system theory; advise on capabilities, limitations, and condition of equipment; implement production control procedures including input/output quality control support; implement and monitor security procedures; perform assigned mission organizational level maintenance and repair of Command, Control, Communications, Computer, and Intelligence Systems" (NAVPERS 18068-67B p. IT-1).

Therefore, an IT cannot focus on one part of his rate, regardless of or in spite of a lack of specialized training. Instead, all of the ITs assigned to a ship are responsible as a whole for all aspects of their rating. Even though ITSN may not completely understand LAN Management, he is expected to know and to perform some LAN-related tasks (e.g., install shipboard personal computers, troubleshoot, and provide basic assistance.)

Herein lies the problem. Ratings require both fundamental knowledge and specialized knowledge as denoted by NECs. However, because an NEC may be specifically associated with a particular rating, then that specialized knowledge is associated with that rating's fundamental knowledge. If IARM were to be taught to an entire rating, there would be those within the rating who would not have immediate cause

to use it. However, if IARM is restricted to certain NECs, then it becomes nothing more than a task-specific tool and not the unifying system it was designed to be.

Consider that IT2 had the time to handle all of the IA technical issues, would ITSN still need IARM? The answer is yes, but not in the same capacity as IT2. ITSN would still be still involved with IA, but as a user and not necessarily as a technical supporter, as some of his radio communication duties entail message dissemination via the ship's LAN. Therefore, even within those ratings identified as being IA technical support-related, personnel can be both users and supporters depending on the task they are performing. Consequently, even though IARM is needed in different ways within a rating (i.e., specialized NEC or general rating duty) and is necessary for both technical support and general users, it does not change the fact that the rating needs IARM.

Because of the dual nature of IARM in the enlisted community, an argument could be made that it is too difficult to establish exactly what point IARM should be taught. However, this argument overlooks the benefits of all concerned with IA knowing IARM. Although IARM aids the technical supporter in performance of his job, it also aids the user in increasing IA awareness and better understanding the technical supporter. In this, its very basic role, it is clear to see that IARM would be beneficial to the entire rating and, therefore, should be taught at the "A" school itself. If an IT does not immediately find himself in a technical supporter role, then at the very least, his "A" school knowledge of IARM would increase his general IA knowledge and help him understand and learn from those ITs who are serving in a technical support capacity. In this capacity, not only does IARM perform its IA role, but also helps the IT rating better impart its general knowledge to its personnel.

3. Putting it all together

Although there are numerous ways to categorize officer and enlisted personnel, how is a ship's manning determined? First, Required Operational Capabilities (ROC) are resolved. These capabilities are the "…functions a ship is expected to perform in order to carry out its assigned mission" (Surface Warfare Officer Schools Command). Next, the Projected Operational Environment (POE) is examined. The POE "…establishes the most demanding environment in which a naval unit must operate and be fully manned and capable of accomplishing its mission" (Surface Warfare Officer Schools Command). The ROC and POE then enable a quantitative and qualitative manpower requirement to be derived for the ship. (It is important to note that because this manning is based on the ROC and POE, it is a wartime manning.) This derived manning requirement then becomes the basis for Manpower Authorization.

The Manpower Authorization (MPA) is not the full manning determined by the ROC and POE, but a quantitative and qualitative requirement for the "peacetime-manning" of the ship (Surface Warfare Officer Schools Command). For the ship's officers, billets are used, and for the enlisted personnel, NECs.

Once the MPA has been established and the appropriate peacetime officer billets and enlisted NECs have been determined for the ship, monthly reports then keep track of the ship's manning. As previously discussed, the EDVR reports the current and future enlisted manning of the ship and summarizes specific rate/NEC shortfalls.

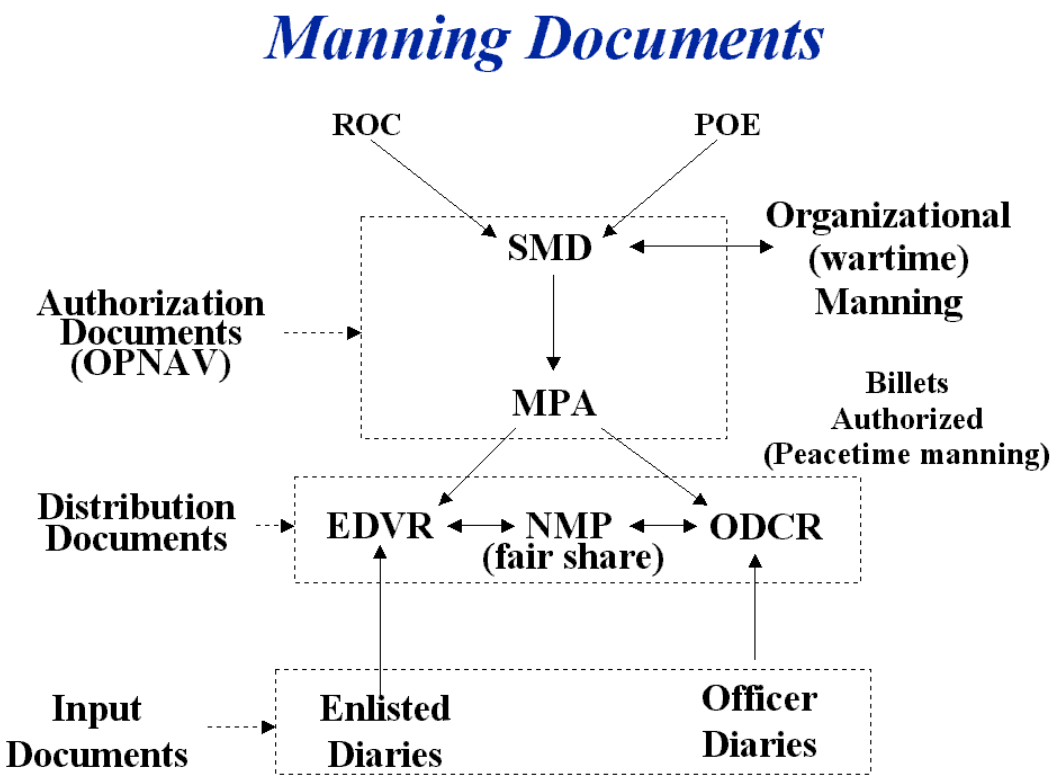

Figure 3-6. "Manning Documents" (From: Surface Warfare Officer Schools Command).

For officers, the Officer Distribution and Control Report (OCDR) functions similarly as the EDVR. Not only do these documents help the ship plan its manning/skill requirements, but they also help the Bureau of Naval Personnel (BUPERS) (who is responsible for overall manning) in assigning the correct personnel to the ship at the right time.

Where does IARM training fit into the overall manning requirements of a ship? The need for IARM has been examined by looking at personnel requirements, billet and rating requirements, and the requirement for general knowledge of IARM itself; however, there is yet another facet which must be discussed. Figure 3-3 ("The Network After

Next") illustrates the DoN desire to evolve toward a network-centric warfare. If a network environment is in the future for the DoN, then a future ship's POE must address IA. If IA is necessary, then a ship's ROC to adequately perform IA also becomes a necessity. If a ship is destined to operate in an IA environment and be capable of performing IA, then IARM training must be inherent to the ship (and therefore all embarked personnel) from the beginning.

D. IMPLEMENTING IARM INTO IT "A" SCHOOL

Exploring the requirements for a TPP and exactly who needs to be taught IARM have already been examined. To fully explore the question as to whether or not IARM can be implemented into existing DoN training pipelines and to stay within the scope of a ship's complement, this section will explore the feasibility of implementing IARM into IT "A" school.

Figure 3-1 illustrates the NETC steps necessary for course development using the PPP method. In keeping with this method, this section will examine the Curriculum Outline of Instruction (COI), which with other documents makes up the Training Course Control Document (TCCD) of Stage 2. The COI will describe the overall course outline and objectives and is the "*…process that directly affects the "teachability" of the course"* (NAVDTRA 131A p. 5-1-1) [emphasis added]. When completed the COI will describe: 1) the overall skills and training to be acquired upon course completion; 2) specific skills and knowledge to be acquired during each topic; 3) organization of subject matter into specific units of instruction and sequence of order; and 4) the developer's

Career Path After Recruit Training Enlistees are taught the fundamentals of this rating through on-the-job training, civilian IT training academies, community colleges or formal Navy schooling. Advanced technical and operational training is available in this rating during later stages of career development.				
School	**Present Location**	**Approximate Training Time**	**Subjects**	**Training Methods**
Class "A" Technical School	Great Lakes, Ill.	Approximately 14 Weeks	Microsoft, Cisco, and Oracle software and hardware fundamentals, ADP, security, system theory and operation	Group instruction, computer lab and ship simulator training.
After "A" school, USN Information Systems Technicians are assigned to all types of ships and shore stations, and to communication stations in the United States and overseas. TAR Information Systems Technicians are assigned to NRF ships in CONUS. Upon completion of sea tours, TAR ITs will be assigned to reserve centers across the country including the heartland. While assigned to reserve centers TAR ITs will train and administer Selected Reserve Personnel. During a 20-year period in the Navy, ITs spend about 50 percent of their time assigned to fleet units and 50 percent to shore stations				

Table 3-1. "Career Path After Recruit Training" (From: "Information Systems Technician (IT)").

intent with respect to the course and each unit of instruction (NAVDTRA 131A p. 5-3-1).

Although NETC is specific as to exactly what criteria are needed for a finished COI, all criteria are not needed for the scope of this discussion. In addition, NETC requires specific formats and codes for its criteria; these, too, will not be used, as they have little value outside of an NETC environment.

1. Course Skills and Training

The PPP method of course development is intended to impart the performance of job skills in the work place to the job standard. Therefore, course skills and training must be derived from the IT rating itself. The overall purpose of IT "A" school is to "… provide the basic knowledge and skills required to enable personnel to perform at the 'job entry' or apprentice level in the IT rating" (CANTRAC). The "skills" and "knowledge" referred to are to "…execute information transfer with state-of-the-art multi-media technology such as fiber optics, digital microwave, and tactical and commercial satellites on a global basis; operate, manage and provide hardware and software support to multi-

media Automated Information Systems (AIS) to include: mainframes, mini, and microcomputers, Local Area Networks (LANs), Wide Area Networks (WANs), and telecommunication; apply diagnostic and restoral techniques utilizing knowledge of electronic and operational system theory; advise on capabilities, limitations, and condition of equipment; implement production control procedures including input/output quality control support; implement and monitor security procedures; perform assigned mission organizational level maintenance and repair of Command, Control, Communications, Computer, and Intelligence Systems" (CANTRAC).

From the very scope of IT "A" school, it is evident that IARM is very applicable. However, by looking at the scope of the course it can also be determined that the addition of IARM would enhance the existing curriculum and therefore does not need to be a stand-alone course for the IT rating. (IARM could certainly be developed into a stand-alone course or training package for those ITs who have not received IARM in "A" school.) Because IARM would enhance the existing course and could be simply added into the curriculum, the current overall course objectives do not need to be altered, but rather merely enhanced.

2. Specific Skills and Knowledge to be Acquired for the IARM Topic

IARM has numerous benefits depending on how it is used. To determine the skills and knowledge for the "A" school, it is important to determine how the IT will use the IARM he is taught. (See "Enlisted" Section 3 "Users and Supporters.")

From the overall scope of the course previously examined, it is clear to see that the IT will use IARM as both a user and technical supporter. However the difference is subtle as the in-depth knowledge of technical supporter-IARM is more than adequate to

also cover user-IARM. By combining the benefits of IARM and the scope of "A" school, it is simple to identify goals for the IARM topic. Therefore the goals of the IARM unit or the specific skills and knowledge an IT should receive from IARM training are:

- Manage information assurance risks to multi-media AIS to include mainframes, mini-, and microcomputers, Local Area Networks (LANs), Wide Area Networks (WANs).
- Identify information assurance assets, procedures, and risks.
- Increase the level of information assurance by identifying potential problems.
- Derive the most cost-effective and efficient corrective controls.
- Assist in advising on capabilities, limitations, and condition of equipment by standardizing the IA syntax.

3. Organization of Subject Matter

Once topic goals are identified, the unit can be organized into a logical progression of topics. LCDR Hernandez proposed topics necessary for the different levels of IARM training. (See Appendix C, Sections A and B.) By arranging these proposed topics into a logical progression of the unit, the following organization can be derived:

- Fundamentals of Information Assurance (IA)
- Basic vulnerability identification, tools, examples
- Vulnerability assessment tools and examples

- Risk assessment tools and examples
- IARM introduction concept
- IARM terms and definitions
- Four principles of IARM
- IARM vs. traditional approach
- Benefits of IARM
- Three levels of IARM
- Time critical IARM, examples, and demonstration
- Deliberate IARM process and demonstration
- Deliberate IARM practical exercise
- Specific applications (demonstrating applicability to existing IA processes and procedures)

4. Developer's Intent with Respect to the Course and Each Unit of Instruction

The goals of the overall course as well as the goals of the IARM section are known. The IARM section can then be broken down into logical units. This section examines the developer's intent for the progression of the course and where exactly each unit would be best integrated to develop this intent.

Again, because IT "A" school is an existing course, the developers intent has already been established. Implementing the IARM units must not affect the original intent of the overall course. To this effect, the placement of the IARM section must be

examined in light of the overall course syllabus and should ensure that the individual units of the IARM section are not repetitive from other sections of the course.

Table 3-2 displays the current IT "A" School computer/network units and topics. By comparing this table to the derived list above of required IARM topics, a logical sequence for the IARM unit and entire curriculum begins to evolve.

Unit 3, Topic 3.1 covers an introduction to Information Systems Security (INFOSEC). In this section, definitions, threat categories, computer vulnerabilities and countermeasures are discussed ("Information Systems Technician 'A' School"). (See Table 3-3.) This section provides the most appropriate place to introduce the topics "Fundamentals of Information Assurance (IA)," "Basic vulnerability identification, tools, examples," "Vulnerability assessment tools and examples," and "Risk assessment tools and examples," as most of the information contained in these topics pre-exists in this section. Although the addition of these IARM topics into Unit 3 would require a small change of the existing material, it is better to integrate IARM topics where applicable than to add a stand-alone IARM unit that may be repetitive of previously-presented topics.

Following Topic 3.1, the introduction of the remaining IARM topics—"IARM introduction concept," "IARM terms and definitions," "Four principles of IARM," "IARM vs. traditional approach," "Benefits of IARM," "Three levels of IARM," "Time critical IARM, examples and demonstration," "Deliberate IARM process and demonstration," "Deliberate IARM practical exercise," and "Specific applications (demonstrating applicability to existing IA processes and procedures)"—could be added

UNIT	TOPIC	TITLE
1	1.1	Introduction to the Information Systems Technician Rating
	1.2	Information Technology for the 21st Century (IT-21) Overview
2	2.1	Introduction to Computers
	2.2	Computer Hardware
	2.3	Computer Software
3	3.1	Introduction to Information Systems Security (INFOSEC)
4	4.1	System Administrator Duties and Responsibilities
5	5.1	Microcomputer Preoperations
6	6.1	Windows NT Environment
	6.2	Preparing for and Installing Windows NT
	6.3	Windows NT Boot Process
	6.4	Windows NT Control Panel
	6.5	Windows NT File System (NTFS)
	6.6	Windows NT Partitions
	6.7	Windows NT Fault Tolerance
7	7.1	Data Communications
	7.2	Introduction to Networks
	7.3	Network Components
	7.4	Introduction to Network Theory
	7.5	Advanced Network Theory
	7.6	Asynchronous Transfer Mode (ATM)
8	8.1	Windows NT Networking Environment
	8.2	Configuring and Installing Protocols
	8.3	Network Browsing—Computer Browser
	8.4	Installing and Configuring WINS and DNS
	8.5	Domains and Creating Computer Accounts in a Domain
	8.6	User and Group Accounts
	8.7	Shared Folder Security
	8.8	Windows NT File System (NTFS) Security
	8.9	Windows NT Printing
	8.10	Backing Up and Restoring Data
	8.11	Configuring and Managing Internet Services
	8.12	Web Browsing
	8.13	Uninstalling Windows NT
9	9.1	Database Fundamentals
	9.2	Microsoft Access
10	10.1	Microsoft (MS) Applications
11	11.1	UNIX Operating System
12	12.1	Navy Networks
13	13.1	Computer Maintenance Fundamentals
	13.2	Microcomputer Troubleshooting and Upgrading

Table 3-2. IT "A" School Computer/Network Curriculum (From: "Information Systems Technician 'A' School").

Unit	Topic	Title
3	3.1	Introduction to Information Systems Security (INFOSEC)
		Introduction
		References
		Information
		1. Threats to Information Systems
		2. Computer Crime
		3. Threats to Security
		4. Computer Vulnerabilities
		5. Countermeasures
		6. Computer Security Incident Reporting

Table 3-3. "Introduction to Information Systems Security (INFOSEC)" Breakdown (From: "Information Systems Technician 'A' School").

as Topic 3.2. (See Table 3-4.) This would ensure a logical flow of the IARM topics added in Topic 3.1 and would provide the least disruption to the remainder of the current curriculum organization. In addition, adding IARM as Topic 3.2 would also make a logical progression into Topic 4.1, which discusses duties and responsibilities of the system administrator and which would greatly benefit from IARM knowledge.

Although it can be argued that topics important to fully understanding IARM (i.e., networks) are not introduced until later in the curriculum, introducing IARM as Topic 3.2 would still be the most logical sequence. An understanding of networks would be beneficial to fully utilizing IARM, but it is not essential for comprehending IARM basics. However, a brief review of IARM and/or more applications of IARM could be included in Unit 7. (It is interesting to note that the only unit that discusses security of any kind is Unit 3. An additional topic on network security (e.g., as Topic 7.7) would be very beneficial and would provide another great place to discuss IARM.)

Unit	Topic	Title	LOs
3	3.1	**Introduction to Information Systems Security (INFOSEC)**	
		Introduction	
		References	
		Information	
		1. Threats to Information Systems	Describe the threats and impacts to information systems.
		2. Computer Crime	
		3. Threats to Security/ Fundamentals of Information Assurance (IA)	Describe prominent information system threats and threat categories. Describe the types of computer vulnerabilities and impact each vulnerability has on IA.
		4. Computer Vulnerabilities/ Basic vulnerability identification, tools, examples	
		5. Countermeasures/Vulnerability assessment tools and examples	Identify the countermeasures used in protecting information systems.
		6. Risk assessment tools and examples	
		7. Computer Security Incident Reporting	
	3.2	**Introduction to IARM**	
		Introduction	
		References	
		Information	
		1. IARM Introduction Concept	Describe the origins of IARM Describe the IARM process.
		2. IARM Terms and Definitions	
		3. Four Principles of IARM	
		4. IARM vs. Traditional Approach	Identify the numerous benefits of IARM.
		5. Benefits of IARM	
		6. Three Levels of IARM	Describe the IARM levels of applications and their associated steps.
		7. Time Critical IARM	
		A. Examples	
		B. Demonstration	
		8. Deliberate IARM Process	
		A. Demonstration	
		B. Practical Exercise	
		9. Specific Applications (demonstrating applicability to existing IA processes and procedures)	Describe how IARM will assist the IT in the Fleet by using applicable examples.

Table 3-4. Proposed "Unit 3" with integrated IARM Topics.

5. Lesson Plans

Figure 3-1 illustrates the NETC steps necessary for course development using the PPP method. In keeping with this method, this section will examine compiling course information from earlier stages into a Lesson Plan, which begins Stage 3. (Development of course materials is suggested for follow-on research; however, the introduction of a basic lesson plan nicely illustrates the complete integration of IARM into an existing curriculum.) According to NAVEDTRA 131A, a lesson plan contains, among other things, "…Learning Objectives (LOs) that reflect the skills and knowledge to be attained upon successful completion of the course" and "…an outline of instructional materials to be taught in a logical and efficient manner" (p. 6-1-1).

Table 3-4 outlines a logical sequence of topics and main points for the proposed Unit 3. Using this sequence of topics and main points, the required outline for a lesson plan also becomes evident. Using Table 3-4 as an outline for the new lesson plan, the following sections identify specific LOs for each topic. (These LOs are a combination of LOs from existing "A" school topics and proposed IARM LOs.)

a. Topic 3.1: Introduction to Information Systems Security (INFOSEC)

The proposed Topic 3.1 is a combination of existing material and new IARM material. Therefore, the original LOs are still applicable but may require the addition of new LOs for the IARM matter. According to IT "A" School the original LOs are:

- Describe the threats to information systems.
- Describe prominent information system threats and threat categories.

- Describe the types of computer vulnerabilities.
- Identify the countermeasures used in protecting information systems.

By grouping the main points identified in Topic 3.1 with their associated LOs (See Table 3-4), the need or lack thereof for additional LOs can be determined. Because Topic 3.1 already contained the same main points as the added IARM material, it becomes evident that the existing LOs are sufficient.

b. Topic 3.2: Introduction to IARM

Topic 3.2 was non-existent before the introduction of the IARM material, so there are no LOs. Using the outline of main points from Table 3-4 and the goals of the IARM unit identified in Section 2, LOs can be determined.

(1) Describe the origins of IARM / 3.2 DESCRIBE the IARM process. These LOs ensure the student is introduced to the IARM concept and process. Using LCDR Hernandez's thesis as reference material, the student becomes indoctrinated into the basics of IARM.

(2) Identify the numerous benefits of IARM. This LO demonstrates the numerous benefits of IARM and its superiority over the traditional method of IA. By identifying the benefits of IARM, the student will realize its usefulness and will be more inclined to incorporate IARM in the future. This thesis and LCDR Hernandez's thesis can be used as reference material.

(3) Describe the IARM levels of applications and their associated steps. This LO ensures that the student is indoctrinated into the different levels of IARM. By introducing the levels of IARM application through demonstrations

and practical exercises, the student will understand that IARM can be applied differently depending on the circumstances. LCDR Hernandez's thesis can be used as reference material.

(4) Describe how IARM will assist the IT in the Fleet by using applicable examples. This LO wraps up the IARM topic and ensures that the student understands that IARM is useful to his future job. Through demonstrations of IARM's applicability to the IA process and IT rate, IARM's usefulness is emphasized. LCDR Hernandez's thesis or personal examples from the instructor can be used as reference material.

E. SUMMARY

Different categorizations of DoN personnel need IARM for numerous reasons. Whether IARM is needed to accomplish a certain job/billet or is fundamentally required for an overall designator/rating, it is evident that there are pre-existing ways of determining who should receive IARM training.

It has also been demonstrated that IARM can be integrated into an existing training syllabus, but can it be integrated into all of the training pipelines Navy-wide? The answer is dependent upon the scale of integration. Because IT "A" school is already teaching INFOSEC, most of the information needed to understand IARM is already present. Therefore certain IARM topics can be directly integrated into existing material, and those topics that cannot still fit logically into existing units. However as previously discussed IARM is not limited to only those training courses related to networks or computer security. Although the purpose of SWOS is to teach new officers to become SWOs (see Section C.1.e of this Chapter), it was demonstrated that the introduction of

IARM into the SWOS curriculum would also be very beneficial to those officers. However, because the SWOS curriculum does not have related information assurance topics, the addition of IARM would therefore necessitate it being a stand-alone unit. Whether directly integrated into existing material, or standing alone as a separate unit in an existing curriculum, the integration of IARM into existing DoN training is beneficial and feasible.

While IARM training can be readily implemented into current training pipelines, it may not be enough. It was established that as the Navy becomes more network-centric, its missions, personnel, and equipment would also become more IA-reliant. Because this is the direction the Navy has chosen, not only will IARM be applicable to those rates identified earlier, but to the entire Department of the Navy. To this end, the Navy must implement IARM in whatever manner that will most easily impact all personnel.

IV. CONCLUSIONS

A. SUMMARY

LCDR Hernandez developed IARM as an answer to the lack of an overall DoN IA strategy. Through the Navy's numerous organizations, overlapping policies, and fragmentation of IA-related personnel, it becomes evident that IARM is still needed. Not only would IARM answer all of the current Navy IA-objectives, but it would also offer the potential to grow and adapt as the Navy's IA needs become more extensive.

The CNO currently requires IA training and, therefore, would also require IARM training should the latter be adopted. Current NETC IA courses do not meet all of the Navy's IA needs. Although these courses do offer some level of IA training, nothing currently exists for all Navy personnel that offers all of the benefits of IARM. Because of this training void, the need for IARM training or an IARM course becomes evident. Though IARM has yet to be adopted, it has been demonstrated that there is enough preliminary NETC-required information to undertake immediate development of such a course.

Looking at the basic categorizations of DoN personnel, it was established that different personnel need IARM for numerous reasons. Whether IARM is needed to accomplish a certain job/billet or is fundamentally required for an overall designator/rating, it is evident that there are existing ways of determining exactly to whom IARM should be taught. By determining who should receive IARM training and why, it became evident that IARM training could easily be implemented into existing training pipelines, such as rating A/C school, billet-specific school, or designator schools.

While IARM training can be readily implemented into current training pipelines, it may not be enough. It was established that as the Navy becomes more network-centric, its missions, personnel, and equipment would also become more IA-reliant. Because this is the direction the Navy has chosen, not only will IARM be applicable to those rates identified earlier, but to the entire Department of the Navy. To this end, the Navy must implement IARM in whatever manner that will most easily impact all personnel.

B. RECOMMENDATIONS

1. Pilot Program

Though IARM would be useful to the DoN as a whole, implementation of a smaller pilot program would be beneficial in demonstrating IARM usefulness and in identifying further areas of IARM study. Figure 3.3 lists a pilot program as one of the NAVEDTRA stages to course development. However, by implementing an "unofficial" pilot program, using nothing more than LCDR Hernandez's thesis and Power Point slides, before the development of a course is actually undertaken, many of the questions this thesis attempted to answer can be more thoroughly derived.

A pilot program aboard a single ship would be easily implemented and beneficial to both the decision makers and technical experts aboard. By giving the Wardroom simple IARM training, it would benefit their abilities to make better decisions concerning IA and IA resources. For the technical experts, such as the ITs and EWs, IARM would increase the general understanding and, consequently, level of IA, increase the understanding of current shipboard IA systems and resources, and identify other ratings or personnel that should also be taught IARM.

Despite the fact that there would be numerous interactions aboard a single ship benefited by IARM, the extent of implementation may not be large enough to fully develop all of IARM's potential. A single ship is one small node in the DoN network; implementation on such a small scale would benefit the node itself, but would provide little data as to IARM benefits for the network as a whole. Perhaps a better pilot implementation would be that of an entire Carrier Battle Group (CVBG) and its associated network operation center (NOC). While the initial training would be greater due to the greater number of people to be trained, it would provide a much more thorough and realistic test of IARM.

2. New Ideas on Training

To be fully applicable to the DoN, Navy publications were used extensively in this research to support current DoN policy and organization. Although it was necessary to work within these boundaries to establish whether or not it was possible to implement IARM, Navy methods of training are not necessarily the best or only way training can be accomplished.

Admiral Vern Clark, the current CNO, has made Navy training and education one of his primary focuses during his tenure. From this focus, numerous studies have examined the outdated way the Navy trains its personnel. As a result, programs such as "Task Force Excel" are attempting to revamp Navy training and produce Navy personnel more aligned to the current and present DoN organization.

Although it was necessary to examine IARM in light of current training and manning policies in order to establish its credibility and necessity to the DoN, IARM training could be a test subject for the CNO's new training ideas. IARM is certainly

necessary for the Fleet and is capable of being taught in existing training pipelines, but why not use a new training method to implement IARM training? Not only would the Fleet be learning something it needs to know, but the Navy would also be able to simultaneously test its training ideas.

C. FUTURE AREAS OF STUDY

LCDR Hernandez's thesis developed the idea of IARM. It was the attempt of this thesis to examine how IARM could be taught Navy-wide. Realizing the importance of IARM, follow-on work in further development of an IARM course would be most beneficial.

1. Naval Education and Training Command Course Requirements

The NAVEDTRA series lists criteria for teaching materials needed for a NETC course or training module. Using these guidelines, further development for IARM training could be studied in development of: 1) management materials, 2) curriculum materials, and 3) support materials.

Developing IARM training material and filling in NETC required information would not only be a worthwhile follow-on thesis, but would also complete another step in actually implementing IARM Navy-wide. (If "Task Force Excel" surpasses the NAVEDTRA manuals, constructing an IARM training course under "Task Force Excel" criteria would also be beneficial.)

2. Pilot Program Study

Implementation of a pilot IARM program would also be interesting follow-on work. Though students at NPS would have a difficult time implementing IARM on a

large scale, they could try to implement IARM at the Postgraduate School itself and study its effects. Though this would be a relatively small-scale program, a successful pilot at NPS could result in excellent exposure for IARM and pave the way for a larger implementation.

A larger pilot program could also be interesting and prove useful as follow-on work. Though a larger pilot-program would have to be sponsored by a larger DoN organization, thesis students could be used to compile results, analyze findings, and make recommendations.

3. IARM in the Department of Defense and the Civilian World

Numerous benefits have been discussed for implementing IARM in the DoN. However, these benefits do not apply solely to DoN assets. Even as the DoN becomes more network-centered, so does the DoD. IARM could provide the same benefits to all of the DoD, thereby increasing IA DoD-wide. Not only would IARM facilitate an increase in IA, but its common language would also facilitate "joint communications," and possibly lead to a truly joint IA policy and organization.

The DoD also realizes that civilian networks are becoming more important as they are becoming more intertwined with those of the DoD. Teaching IARM to civilians would also benefit National IA, as the entire infrastructure would now be speaking the same language. Though implementation of IARM in DoD and civilian networks would be difficult to study, it would nonetheless prove to be an enormous benefit.

D. FINAL COMMENTS

While it was necessary to distinguish between users and supporters, and officers and enlisted, to illustrate the necessity for IARM and where and how it may be properly implemented in the DoN, it may have inadvertently caused an even greater peculiarity between the groups. IARM, by its very nature, strives to eliminate distinctions.

Although there is a different knowledge requisite between users and technical supporters, and hence a need for either training or education, it does not necessarily have to impact IARM directly. IARM is designed to be a stand-alone process that facilitates information assurance risk management for whomever uses the process regardless of the level of their IA education or training. The IARM process is designed to be simple enough for a user to understand the risks involved without actually having to understand the technical background, yet robust enough to allow the technical supporter to better perform his job. In fact, the DoN organization itself has already designated who will be a user and who will be a technical supporter and to that end provided the appropriate level of either background training or education. Perhaps a stand-alone IARM class is not as necessary as is simply incorporating IARM training into existing designator, rank, billet, or rating schools.

IARM strives to bring the user and technical supporter together, so an IARM training course should not differentiate between the two. It is important to remember that as the Navy becomes more network-centric, more and more DoN personnel will have to become network users. Even basic users would benefit from IARM training. To this end, IARM turns once more to the vision of its cousin ORM; "the naval vision is to

develop an environment where *every* [emphasis added] leader, Sailor, Marine and civilian is trained and motivated to personally manage risk in everything they do, both in peacetime and during conflict, thus successfully completing all operations with minimum risk" (OPNAV INSTRUCTION 3500.39A p. 2). To accomplish this ORM vision, the Navy simply stated, "ORM will be included in the orientation and training *of all military personnel*" (OPNAV INSTRUCTION 3500.39A p. 2) [emphasis added]. Why reinvent the wheel? IARM is to Information Assurance as ORM is to Operations. Adopt IARM training for all Navy personnel.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. NAVY INFORMATION ASSURANCE (IA) PROGRAM

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

IN REPLY REFER TO

OPNAVINST 5239.1B
N6
9 November 1999

OPNAV INSTRUCTION 5239.1B

From: Chief of Naval Operations
To: All Ships and Stations (less Marine Corps field addresses not having Navy personnel attached)

Subj: NAVY INFORMATION ASSURANCE (IA) PROGRAM

Ref: (a) SECNAVINST 5239.3 of 14 Jul 95, Department of the Navy Information Systems Security (INFOSEC) (NOTAL)
(b) DoD 5220.22-M of January 95, National Industrial Security Program Operating Manual (NISPOM)
(c) Public Key Infrastructure Roadmap for the Department of Defense, Version 2.0, Revision C, June 15, 1999
(d) CNO N64 Attack, Protect, Exploit Requirements Action Forum Charter
(e) Department of the Navy Chief Information Officer Information Technology Standards Guidance (ITSG) (NOTAL)
(f) DoD Instruction 5200.40 of 30 Dec 97, Department of Defense Information Technology Security Certification and Accreditation Process (NOTAL)
(g) CNO Memo 1500 Ser N7/8U637313 of 14 Oct 98 (Subj: Navy Communications, Information Systems, and Networks (CISN) Training Strategy to Support Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance/Information Operations (C4ISR/IO)) (NOTAL)
(h) NSTISSI No. 4012, of August 1997, National Training Standard for Designated Approving Authority (DAA) (NOTAL) (i) OPNAVINST 2201.2 of 3 March 1998, Navy and Marine Corps Computer Network Incident Response

Encl: (1) List of Acronyms

1. Purpose. To establish policies and procedures for the U.S. Navy's Information Assurance (IA) Program, and implement the provisions of reference (a). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. OPNAVINST 5239.1A.

3. Applicability. This instruction applies to all Navy activities, organizations and contractors that enter, process, store, or transmit unclassified, sensitive but unclassified (SBU) or classified National Security information using information systems or networks at Navy activities, and to contractor operated or owned facilities under Navy authority, which shall also comply with the guidelines of reference (b). This instruction encompasses all information systems and networks that are procured, developed, modified, operated, maintained, or managed by Navy organizational elements. If information in this policy conflicts with other issued policy, the more stringent policy applies. Enclosure (1) provides a list of acronyms used throughout this instruction.

4. Background

a. Information Assurance is defined in Joint Pub 3-13 "Joint Doctrine for Information Operations" (9 October 1998) as:

"Information operations that prOteCt and defefl information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes prwiding for restoration of information syeteme by incorporating Protection, detection, and reaction capabilities."

b. The security challenges confronting Navy information and information systems are multiplying rapidly with the exponential growth of interconnected systems for producing and exchanging data and information. As intercomectivity increases and the threats to information and information systems become more sophisticated and diverse, Navy systems become inherently more vulnerable to surreptitious access end malicious attacks.

The fast-paced advances of technology drive Navy reliance on commercial technologies and services; however, many of these solutions may offer only minimal defense against IA threat activity and must be augmented by IA disciplines and focused management decisions to ensure protection of Navy information and information systems.

c. Information Assurance Properties and Services. Information and information systems must be properly managed and protected as required by law, regulation or treaty. Facilitating the management and protection of resources requires the appropriate implementation of security measures providing the IA properties and services of:

(1) Confidentiality, which supports the protection of both sensitive and classified information from unauthorized disclosure.

(2) Integrity, which supports protection of information against unauthorized modification or destruction.

(3) Availability, which supports timely, reliable access to data and information systems for authorized users, and precludes denial of service or access.

(4) Authentication, which supports verifying the identity of an individual or entity and the authority to access specific categories of information.

(5) Non-repudiation, which provides assurance to the sender of data with proof of delivery and to the recipient of the sender's identity, so that neither can later deny having processed the data.

d. Mission Criticality. Assessing the security requirements of any information system for the five IA properties requires a determination of the criticality of the information system to the organization's mission, particularly the warfighter's combat mission. Five categories of criticality are defined in reference (c), Administrative, Mission Support, and three categories classified as Mission Critical, although an information system may have components that fit in more than one category. Mission criticality is one of the key determinants of

information security requirements, the level of effort appropriate to the certification and accreditation of systems, and the technologies appropriate for implementing the required safeguards.

e. Information Sensitivity. Information Assurance requirements also depend on the need to control disclosure. Disclosure may be restricted either because of national security classification levels (Confidential, Secret, Top Secret), because of Special Access (Single Integrated Operations Plan — SIOP -- or Sensitive Compartmented Information — SCI) requirements, or for other sensitivity. Sensitive information is any information the loss, misuse, or unauthorized access to, or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy of Department of Defense personnel, but that has not been specifically authorized to be kept classified. Unclassified national security information, Privacy Act data, personal information (such as medical records, fitness reports and performance evaluations), proprietary, source selection sensitive, nuclear propulsion information, operations or mission information may be considered sensitive information.

5. Objectives. The Chief of Naval Operations directs the implementation of the Navy IA program, through the policy set forth in this instruction, to:

a. Protect information and resources to the degree commensurate with their value.

b. Employ efficient procedures and cost-effective, information-based security features on all information technology resources procured, developed, operated, maintained, or managed by Navy organizational elements to protect the information on those resources. An analysis of costs and benefits should be used determine which procedures and security features are appropriate, including a realistic assessment of the remaining useful life of legacy systems compared with the cost of adding new security safeguards.

c. Adopt a risk-based life cycle management approach in applying uniform standards for the protection of Navy information technology resources that produce, process, store, or transmit information.

d. Conduct an assessment of threats, identify the appropriate combination of safeguards from the IA disciplines, and apply an appropriate level of certification and accreditation for each specific information system developed by a program office and for each site employing networks and deployed information systems.

6. Policy. All Navy information and resources shall be appropriately safeguarded at all times, to support defense-indepth across Navy and DoD. Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, authentication, and non-repudiation based upon mission criticality, level of required information assurance and classification or sensitivity level of information entered, processed, stored, or transmitted. The safeguarding of information and information systems shall be accomplished through the employment of multi-disciplined defensive layers, as well as sound administrative and operational practices.

7. IA Requirements. IA Requirements should be validated by the Fleet Commanders-in-chief or other Echelon II Commanders and forwarded to the CNO N64 Attack/Protect/Exploit (CAPER) Action Forum, via CNO N643. The principle mission of the CAPER Action Forum is to review, clarify, define and validate certain CNO sponsored program issues and requirements for the operating forces of the United States Navy.

8. Information Assurance Publications. The IA Publication series provide specific guidance and direction on implementation of this instruction for Navy, and as such, are extensions of the policies herein. The IA publications detail specific roles and responsibilities and reflect the latest affordable, acceptable, and supportable procedures and products to ensure the security and protection of Navy information. IA Pub 01 introduces and summarizes the Department of the Navy's approach to IA. Pub 01 is intended to foster a common understanding of IA principles, concepts, and interrelationships among system planners,

organizational managers, Information Systems Security Officers and Managers, and users. Appendix A to IA Pub 01 lists and describes the current and planned IA Pubs. The IA publications are maintained by Director, Communications Security (COMSEC) Material System (DCMS) and shall be updated routinely. The IA Pubs are available on the NIPRNET and the SIPRNET at the INFOSEC Web Site.

9. Responsibilities

a. Organizational Responsibilities.

(1) Chief Of Naval Operations (CNO). The CNO is responsible for ensuring full implementation and coordination of Navy IA Program execution with the Assistant Secretary of the Navy (ASN) Research Development & Acquisition (RD&A) and Deputy Assistant Secretary of the Navy (DASN) Command, Control, Communications, Computers and Intelligence/Electronic Warfare/Space (C4I/EW/Space). The CNO executes this responsibility by:

(a) Appointing the Navy Senior Information Systems Security Manager (SISSM) with authority as the Navy principal Designated Approving Authority (DAA) for collateral/GENSER classified and sensitive but unclassified information systems.

(b) For the Navy, the CNO has appointed the Director, Space, Information Warfare, Command and Control (N6) as the SISSM. (c) CNO (N6) has delegated the duties of Navy SISSM to CNO (N643).

(d) Directing the SISSM to ensure execution of responsibilities outlined in reference (a) and to develop the procedures and policies necessary to implement higher directives and regulations.

(e) Appointing CNO (N89) as the DAA for all Special Access Programs.

(f) Appointing CNO (N3/N5) as the DAA for all Single Integrated Operations Plan (SIOP) programs.

(g) Appointing Director, Office of Naval Intelligence as the DAA for all Sensitive Compartmented Information (SCI) programs.

(h) Appointing Commander, Naval Security Group Command as the DAA for all cryptologic systems and SCI physical facilities under their cognizance.

(2) CNO (N643) shall:

(a) Oversee the Navy IA Program. Provide streamlined, simplified and standardized security guidance and policy.

(b) Approve and issue the Navy IA Master Plan.

(c) Represent IA Requirements submitted by Fleet Commanders-in-Chief and other Echelon II Commanders to the CNO N64 Attack, Protect, Exploit Requirements Action Forum (CAPER AF) (ref (d)).

(d) In coordination with Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) (PMW-161), develop and issue standards for critical IA components (e.g. firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs)), for use within Navy information systems and networks. Critical IA components are those which, to ensure interoperability with other Navy, joint or other DoD systems, must be standardized and managed at a service level. Standards will be documented in the DoN CIO Information Technology Standards Guidance, Chapter 3 (ref (e)).

(e) Represent CNO as the DAA for Navy-wide and joint service information systems (where Navy is the assigned lead). Assign DAAs and ensure the accreditation of all Navy information technology resources. CNO (N643) further delegates DAA authority to second echelon commanders for acquisition and development of information systems within their cognizance. Further delegation of this DAA authority is limited to officers of the grade of O-6 or above and civilians of grade GS-15 or equivalent except by prior coordination with and authorization from CNO (N643).

(f) Provide Navy representation to the DoD Information Assurance Panel, subordinate working groups and other DoD-level working groups and study groups relating to IA.

(g) Coordinate Navy submission of reports on IA postures, to include training initiatives and overall progress in meeting IA goals and objectives.

(h) Oversee Navy IA training requirements and provide requirements to the Communications, Information Systems, and Networks (CISN) Training Working Group (see item (7)).

(3) Commander, Space and Naval Warfare Systems Command (COMSPAWARSYSCOM) (PMW-161) is the Department of the Navy's IA Program Manager. As such COMSPAWARSYSCOM (PMW-161) shall:

(a) Ensure full coordination of Navy IA program execution with CNO (N643), COMNAVSECGRU, COMSPAWARSYSCOM (PMW- 162) and Headquarters USMC.

(b) Draft and maintain the Navy IA Master Plan as requested by CNO (N643), and in coordination with CNO N64 Attack/Protect/Exploit Requirements (CAPER) Action Forum, Headquarters Marine Corps, COMNAVSECGRU, and other Naval Systems Commands. The IA Master Plan shall include identification and formal documentation of IA goals and objectives for Navy, a strategy for achieving those goals and objectives, a description of IA programs, projects and initiatives that will result in the capabilities needed, and an IA risk management plan. The Navy IA Master Plan and updates as required will be submitted to CNO (N643) for approval and issuance.

(c) Submit Program Objectives Memorandum (POM) requirements to support IA programs as delineated in the Navy IA Master Plan.

(d) Execute Navy IA programs as defined in the Navy IA Master Plan.

(e) As the technical lead for Navy IA, provide systems and security engineering and integration testing and support for Navy information systems and networks with IA requirements. Provide input, review, and recommended updates to IA Publications. Establish and execute capability to provide on-site assessments to Navy commands, including vulnerability assessments coordinated by FIWC.

(f) Maintain a Navy IA research and development program to meet Navy requirements in accordance with the Non- Acquisition Program Decision Document (NAPDD) and as delineated in the Navy IA Master Plan. Coordinate IA R&D activities with the Office of Naval Research to ensure maximum and smooth transition of new technologies to operating forces, fully integrated for maximum cost effectiveness with existing technologies.

(g) As the Navy's Certification Authority:

1. Provide high-level oversight and standardization for the system certification and accreditation process for all Service, Joint, development and acquisition programs across Navy.

2. Advise program managers and DAAs in their responsibility to assign a capable Certification Agent responsible for completing the certification and accreditation process in accordance with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP), reference (f).

3. Establish and maintain a master file of Navy accredited systems and major network operations centers (NOCs). Ensure supporting certification and accreditation documents are analyzed for lessons learned, identification of system deficiencies and for incorporation in process improvements and the Navy IA Master Plan.

(h) Develop and centrally acquire Navy standard and specified IA products. Provide life cycle management support for centrally procured IA products and systems, to include operations and maintenance funding.

(i) Maintain the Navy INFOSEC Web Site and IA Help Desk as directed by CNO (N643).

1. Navy INFOSEC Web Site. The Navy INFOSEC Web Site on the World Wide Web provides access to the Navy IA Publications, as well as other IA related references, advisories and announcements, and a variety of resources on IA issues across Navy, the Department of Defense and other services and agencies. The INFOSEC Web Site URL on the Non-classified Internet Protocol Router Network (NIPRNET) is http://infosec.navy.mil/. On the Secret Internet Protocol Router Network (SIPRNET) the URL is http://infosec.navy.smil.mil/.

2. Information Assurance Help Desk. For routine technical and engineering assistance, an IA Help Desk has been established under COMSPAWARSYSCOM (PMW-161) to support Navy and Marine Corps commands on IA matters and provide guidance on specific questions for securing and certifying systems. The Help Desk is available at 1-800-304-4636.

(j) Support Navy Computer Network Defense by providing network analysis and management tools to support the Navy Component Task Force – Computer Network Defense (NCTF-CND) mission.

(4) COMSPAWARSYSCOM (PMW-162) shall conduct IA Vulnerability Assessments in support of the DITSCAP Certification and Accreditation process for developing systems.

(5) Commanders of Systems Commands and other Navy development and acquisition activities shall ensure Program Managers integrate information assurance requirements in the design of information systems and that all systems are delivered to naval customers with certification documentation to support accreditation requirements of ref (f).

(6) Commander, Naval Security Group Command (COMNAVSECGRU) shall:

(a) Serve as DAA for accreditation of Cryptologic systems and networks. Coordinate the Navy Service Cryptologic Element (SCE) program with the National Security Agency (NSA).

(b) Serve as DAA for SCI physical facilities under COMNAVSECGRU cognizance.

(c) Provide support, as coordinated by FIWC, in the conduct of vulnerability assessments and Red and Blue Team operations.

(7) The Communications, Information Systems, and Networks (CISN) Training Working Group, established under reference (g), shall:

(a) Identify Navy IA billet and training requirements.

(b) Ensure development of Navy training plans for information systems.

(c) Establish IA training requirements for military and civilian personnel.

(8) Chief of Naval Education and Training (CNET) shall:

(a) Develop Navy schoolhouse IA training and education.

(b) Ensure IA training is incorporated into all pertinent Navy training and appropriate formal schools.

(9) Fleet Information Warfare Center (FIWC) shall:

(a) Manage the Naval Computer Incident Response Team (NAVCIRT) for Navy; The NAVCIRT, located at FIWC, serves as the Navy primary computer incident response capability to provide assistance in identifying, assessing, containing, and countering incidents that threaten Navy information systems and networks. On request NAVCIRT will offer hands-on assistance to selected naval activities, such as deployed ships, that are under cyberattack. FIWC will collaborate and coordinate Navy efforts with other Government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and information systems, and to minimize or eliminate identified vulnerabilities.

(b) Provide CNO (N64) with monthly, quarterly, and annual summaries of reported Navy computer incidents.

(c) Provide timely advisories of newly identified vulnerabilities.

(d) Conduct on-line surveys for fielded systems.

(e) Provide vulnerability assessments and Red and Blue Team operations to requesting commands. Coordinate resources provided by COMNAVSECGRU and COMSPAWARSYSCOM PMW-161 as required.

(f) Provide intrusion detection monitoring, on-line surveys, and activity analysis and assessment in support of the NCTF-CND (see item 13).

(10) Director, Office of Naval Intelligence (ONI) shall:

(a) Coordinate Navy IA requirements for the Navy SCI/Intelligence program and the Navy portion of the DoD Intelligence Information System (DODIIS) with the Defense Intelligence Agency (DIA).

(b) Serve as DAA for Navy SCI systems.

(c) Assist CNO (N643) and COMSPAWARSYSCOM (PMW-161) by gathering relevant threat information to assist in defining system security requirements.

(d) Provide all-source, fused intelligence support to the NCTF-CND (see item 13).

(11) Commander, Naval Computer and Telecommunications Command (NCTC) shall:

(a) Coordinate Defense Information Infrastructure (DII) connection approval with the Defense Information Systems Agency (DISA) for Navy information systems and sites. Ensure sites with DII connections meet DISA accreditation requirements.

(b) As required, provide Internet web-hosting and demilitarized zone (DMZ) services for afloat units and small shore commands. A DMZ is a dedicated network segment that is used to separate public services from internal services.

(c) Ensure shore-based infrastructure solutions incorporate appropriate IA safeguards.

(d) Provide network operations, including monitoring and restoral functions in support of the NCTF-CND (see item 13).

(12) Director, COMSEC Material System (DCMS) shall:

(a) Maintain Central Office of Record (COR), ensuring the proper storage, distribution, inventory, accounting, and overall safeguarding of COMSEC materials for the Navy, Marine Corps, and Coast Guard, Military Sealift Command, and joint and allied commands, as required.

(b) Maintain the IA Publication Library as directed by CNO (N643).

(c) Control, warehouse, and distribute cryptographic equipment, ancillaries and associated keying material for all Navy.

(d) Under CNO (N643) direction, issue, publish and distribute guidance necessary to ensure National level (e.g., NSA) policies are followed and enforced.

(e) Act as the Navy High Assurance (Class 4) PKI Certificate Approving Authority. Communications Security (COMSEC) Material Issuing Office (CMIO) Norfolk provides a Navy Centralized CAW Facility (NCCF) to support DMS for other than Organizational Messaging and non-DMS FORTEZZA® requirements.

(f) Act as Navy Registration Authority for Medium Assurance (Class 3) PKI.

(13) Navy Component Task Force – Computer Network Defense (NCTF-CND) shall:

(a) Coordinate the defense of Navy computer networks and systems as directed by the Commander, Joint Task Force for Computer Network Defense (JTF-CND).

(b) Defend computer networks and systems within the Navy's elements of the Defense Information Infrastructure, as directed by the JTF-CND.

(c) When tasked, be responsible for the monitoring, restoral, and security of Navy networks.

(d) Monitor the Navy's Information Assurance Vulnerability Alert (IAVA) compliance and act as the Navy's Reporting Agent for IAVA.

(e) Coordinate/direct appropriate actions to ensure Navy web pages resident on the World Wide Web are in compliance with prescribed Department of Defense and Navy guidance.

(f) Make Information Operations Condition (INFOCON) recommendations to the Navy Command Center in response to a Computer Network Attack and report the Navy INFOCON status.

(14) Naval Criminal Investigative Service (NCIS) shall provide law enforcement and counter-intelligence support to the NCTF-CND and FIWC.

b. Individual Responsibilities

(1) Fleet Commanders-in-Chief and Second Echelon Commanders are responsible for implementation of the Navy IA Program within their respective claimancies and areas of responsibility and shall:

(a) Appoint in writing an Information Assurance Officer to oversee and provide IA guidance to subordinate organizations.

(b) Appoint in writing an Information Systems Security Manager (ISSM) to oversee and implement the IA program within the claimancy. This may be, but need not be the same individual assigned as Information Assurance Officer.

(c) Provide oversight and management of the activity IA training program in accordance with all policies stated and referred to by this instruction, to include the Navy IA Publication Library.

(d) Request vulnerability assessment assistance and Red and Blue Team operations from FIWC to validate IA controls and practices.

(2) Commanding officers, commanders, and officers-incharge are responsible for the overall management of IA at the command level and shall:

(a) Ensure all automated information systems or networks used by the command are individually and collectively accredited by the site DAA, or by the appropriate DAA in the case of information system services centrally procured or provided by another command.

(b) Ensure that all of the requisite safeguards, as documented in the respective System Security Authorization Agreement (SSAA), are implemented and that the site maintains accreditation. Assess the need to reaccredit with each system configuration change. While it is expected that the commander will be assisted in this effort by a certification agent, ISSM or Information System Security Officer (ISSO), accreditation is considered a command responsibility.

(c) Appoint, in writing, an ISSM. Where management and administrative functions have been consolidated within a Navy organization, the higher-level organization head may designate a single ISSM to manage IA for the entire organization, and subordinate ISSMs need not be appointed.

(d) Ensure that an ISSO is designated, as appropriate, for each information system and network in the organization, responsible for implementing and maintaining the site's information system and network security requirements. For smaller commands, the same individual may perform ISSM and ISSO duties.

(e) Ensure current standard operating procedures; inclusive of IA practices and procedures, are available and used for all information technology resources.

(f) Ensure IA awareness indoctrination and annual IA refresher training are conducted down to the user level, tailored to specific site requirements.

(g) Ensure all personnel performing IA functions receive initial basic and system specific training, required certification, as well as annual recurring, refresher, or follow-on training.

(h) Ensure any computer intrusion incident, or suspicion of one, is reported to FIWC at navcirt@fiwc.navy.mil or 1-888-NAVCIRT, as required by reference (i).

(3) Designated Approving Authority (DAA). General guidance on DAA roles and responsibilities is available in ref (h). Whether fulfilling the duties as DAA for program or systems development or as a site DAA, all DAAs shall:

(a) Ensure sites and systems under their cognizance are accredited in accordance with the DITSCAP (reference (f)). In doing so they shall review certification documentation to evaluate and determine an acceptable level of risk for information systems and for overall site configuration, to include the aggregate of information technology resources employed in a given geographic locale.

(b) Ensure accredited sites and systems maintain the approved security posture throughout the life cycle.

(c) Ensure the respective SSAA delineates the applicable IA training requirements for users, operators, maintainers, administrators, and managers in accordance with this instruction and all specified references. Site DAAs shall ensure the training requirements delineated in the SSAA are met and that training requirements for specific roles (e.g., DAA, ISSM, ISSO) are met prior to appointment.

(d) Coordinate any requirements for delegation of DAA authority with CNO (N643).

10. Action. All action addressees shall implement the guidance contained herein and all associated references to include the Navy IA Publication Library. All developing and operating activities shall budget for, fund and execute the actions necessary to comply with this instruction and the publications that support it.

R. W. MAYO
Rear Admiral, U.S. Navy
Director,
Space, Information Warfare,
Command and Control (N6)

Distribution:
SNDL Parts 1 and 2

LIST OF ACRONYMS

AIS:	Automated Information System
ASN:	Assistant Secretary of the Navy
C&A:	Certification and Accreditation
CIO:	Chief Information Officer
COMSEC:	Communications Security
COR:	Central Office of Record
DAA:	Designated Approving Authority
DASN:	Deputy Assistant Secretary of the Navy
DCMS:	Director, COMSEC Material System
DIA:	Defense Intelligence Agency
DII:	Defense Information Infrastructure
DITSCAP:	Defense Information Technology Security C&A Program
DoD:	Department of Defense
DoN:	Department of the Navy
FIWC:	Fleet Information Warfare Center
FLTCINC:	Fleet Commander-in-Chief
GENSER:	General Services
IA:	Information Assurance
IAAV:	Information Assurance and Assist Visit
INFOSEC:	Information Systems Security
ISSM:	Information Systems Security Manager
ISSO:	Information Systems Security Officer
NAVCIRT:	Naval Computer Incident Response Team
NIPRNET:	Non-classified Internet Protocol Router Network
NISPOM:	National Industrial Security Program Operating Manual
NOC:	Network Operations Center
OLS:	On-line Survey
ONI:	Office of Naval Intelligence
PKI:	Public Key Infrastructure
RD&A:	Research, Development and Acquisition
SABI:	Secret and Below Interoperability
SBU:	Sensitive but Unclassified
SCE:	Service Cryptologic Element
SCI:	Sensitive Compartmented Information
SIOP:	Single Integrated Operations Plan
SIPRNET:	Secret Internet Protocol Router Network
SISSM:	Senior Information Systems Security Manager
SPAWAR:	Space and Naval Warfare Systems Command
SSAA:	System Security Authorization Agreement
URL:	Universal Resource Locator

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. INFORMATION ASSURANCE RISK MANAGEMENT PROCESS (HERNANDEZ P. 41-47)

E. IARM PROCESS

The IARM process is a simple five-step process. It is a continuous process designed to detect, assess, and control risk to information while qualitatively enhancing computer network defense (CND) performance and maximizing network capabilities. It is adapted from the concept of applying a standard, systematic approach to minimizing risk that was originally developed to improve safety in the development of weapons, aircraft, space vehicles, and nuclear power and is used throughout the Navy in Operational Risk Management (ORM). The five steps are:

1. Identify Vulnerabilities

Identify potential causes of compromise to information in terms of confidentiality, integrity, and availability. Specific actions include identifying computer network assets and listing vulnerabilities in terms of its effects on security services. Assets can include hardware, software, data, services, people, documentation, policies and supplies. (Pfleeger, p. 464) A table, as shown in Table 3-1 [Table A-1], can be used to organize the association of vulnerabilities and assets.

ASSET	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Hardware			
Software			
Data			
Services			
People			
Policies			
Documentation			

Table B-1. "Assets and Security Services (After Pfleeger)" (From: Hernandez p. 42)

2. Asses Vulnerabilities

For each vulnerability identified, determine the associated risk in terms of severity and probability. Specific actions include assessing the exposure, severity and probablility to the vulnerabilities listed in step 1. The Risk Assessment Code (RAC) chart in figure 3-3 [Figure A-1] can be used to accomplish this step.

Risk Assesment Code-
(RAC)
1 = Critical
2 = Serious
3 = Moderate
4 = Minor
5 = Negligible

CAT I = Catastrophic consequences
CAT II = Severe consequences
CAT III = Minor consequences
CAT IV = Minimal consequences

		Probability of Occurrence			
		Likely-Immediate	Probably will occur in time	May occur	Unlikely to occur
		A	B	C	D
SEVERITY	CAT I	1	1	2	3
	CAT II	1	2	3	4
	CAT III	2	3	4	5
	CAT IV	3	4	5	5

Risk Levels
Risk Assesmnet Code

Figure B-1. "IARM Risk Assessment Code Chart (After U.S. Navy & Marine Corps School of Aviation Safety ORM Presentation)" (From: Hernandez p. 43)

Using this matrix does not lessen the inherently subjective nature of risk assessment, however a matrix does afford a consistent framework for evaluating risk. Although different matrices may be used for various applications, any risk assessment tool should include the elements of vulnerability severity and threat probability. The RAC defined by a matrix represents the degree of risk associated with a vulnerability considering severity and probability. While the degree of risk is subjective in nature, the RAC does accurately reflect the relative amount of risk perceived between various vulnerabilities. Using the matrix, the RAC is derived as follows:

a. Vulnerability Severity – An assessment of the worst credible consequences that can occur as a result of a vulnerability. Severity is defined by a potential degree of information compromise, or loss of information all together (e.g.

denial of service). The combination of the two or more vulnerabilities may increase the overall risk. Vulnerability categories are assigned as Roman numerals according to the following criteria:

(1) Category I – The vulnerability may cause catastrophic loss of information or grave damage to national interests.

(2) Category II – The vulnerability may cause severe loss of information, severe damage to national or service interests, or severe degradation to the efficient use of information.

(3) Category III – The vulnerability may cause minor loss of information, minor damage to national, service or command interests, or minor degradation to efficient use of information.

(4) Category IV – The vulnerability may cause a minimal loss of information, minimal damage to national or service interests, or minimal degradation to efficient use of information.

b. Exploitation probability – the probability that a vulnerability will result in an actual exploitation (some degree of compromise of data or denial of service), based on an assessment of such factors as location, exposure, affected population, experience, or previously established statistical information. Exploitation probability will be assigned an English letter according to the following criteria:

(1) Sub-category A – Likely to occur immediately or within a short period of tme. Expected to occur frequently to a computer network, servers, host or client.

(2) Sub-category B – Probably will occur in time. Expected to occur several times to a computer network, server, host or client.

(3) Sub-category C – May occur in time. Can reasonably be expected to occur sometime to a computer network, server, host or client.

(4) Sub-category D – Unlikely to occur.

c. Risk Assessment Code – The RAC is an expression of risk that combines the elements of vulnerability severity and exploitation probability. The RAC is expressed as a single Arabic numeral that can be used to help determine vulnerability control priorities. Note that in some cases, the worst credible consequence of a vulnerability may not correspond to the highest RAC for that vulnerability. For example, one vulnerability may have two potential consequences (loss of confidentiality – I and non-repudiation – III). The severity of the worst consequence (loss of confidentiality) may be unlikely (D), resulting in RAC 3. The severity of the lesser consequence (III) may be likely (A), resulting in a RAC of 2. Therefore, it is also important to consider less severe consequences of a vulnerability if it is more likely than the worst credible consequence, since the combination may present the greater overall risk. (OPNAVINST 3500.39, p. 7)

3. Make Risk Decisions

Develop risk control options, and then decide if benefits outweigh risks. Start with the most serious risk first. Specific Actions include identifying control options, determining the effects of those controls, prioritizing risk control measures, selecting risk controls and making risk decisions. If risks outweigh benefit, or if

assistance is required to implement controls, seek further controls or guidance from superiors.

4. Implement Controls

Once the risk decisions are made, implement selected controls. Specific actions include making implementation of the above controls clear, establishing accountability, and providing support. If the control entails a new IT technology like implementing a Virtual Private Network (VPN) for network traffic confidentiality, then it is vital that an investment be made into the people who will maintain and use it as well. A grouping of controls can be as follows:

a. Controls that implement confidentiality, integrity, authentication and non-repudiation: Public Key Infrastructure (PKI), secure protocols (IPSec), secure e-mail (PGP), network integrity controls (intrusion detection systems), operating system protection features (anti-virus software), Secure Shell (SSH), etc. These controls are most applicable to implementations at the application level

b. Controls that implement availability and access controls: network access controls (firewalls), secure socket layer (SSL), identification, database and operating system access controls, etc. These controls are most applicable to implementations at the transport and network levels.

c. Controls that protect the physical medium of transmission: link cryptography, spread-spectrum (low probability of detection and interception techniques (LPD and LPI)), etc. These controls are most applicable to the physical and data link levels.

5. Supervise

Some methods of testing must be devised to ensure that the selected controls are performing as needed. A well-designed vulnerability assessment can satisfy this need. Care must be taken to watch for changes that could impact the original assumptions of the risk assessment. A change of this nature usually warrants initiating the IARM process again. Other specific actions include supervising the control implementation, continuously monitoring for effectiveness, and collecting feedback from non-involved IT support personnel and users. A summary of specific actions associated with each step of the IARM process is given below in figure 3-4 [Figure A-2].

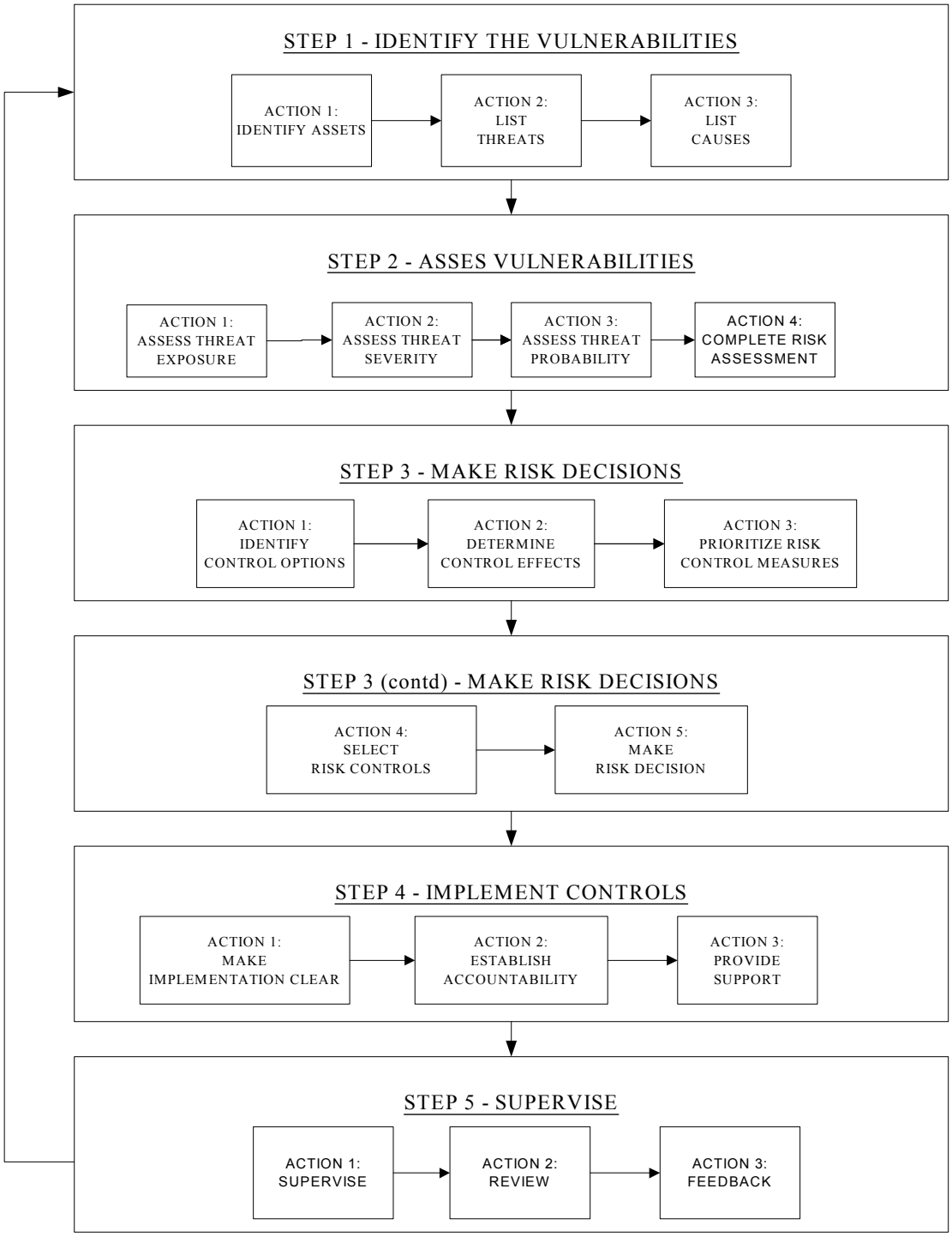

Figure B-2. "The Cyclic IARM Process (After U.S. Air Force ORM Process)" (From: Hernandez p. 47)

APPENDIX C. PROPOSED INFORMATION ASSURANCE RISK MANAGEMENT (IARM) CURRICULA (HERNANDEZ, P. 69-75)

The Naval Postgraduate School (NPS) has many areas of academic excellence that can be brought together to promote IA in the DON. The Center for Information Systems Security Studies and Research (CISR) is already an acknowledged center of excellence in the field of computer security. The Center for Executive Education (CEE) holds Flag-level seminars on revolutionary business practices and enjoys an excellent reputation among the senior leadership of the Navy. The Information Warfare systems engineering curriculum is active in developing different taxonomies of Information Operations (IO). IA can most benefit from a multi-disciplinary approach that includes computer science, information technology management, organizational behavior and Information Operations. These areas can be combined into an "Institute for Information Security (IIS)." This center can study how information has become the center of gravity for many functions in today's world and the future. From business commerce to military operations, information, and its unhampered distribution, is seen as the key competitive edge needed to gain the advantage in many confrontational and competitive situations. How that information is managed, protected and distributed can be the focus of such a center. Also, similar to the U.S. Navy and U.S. Marine Corps School of Aviation Safety and the Naval Safety Center and their positions as the standard-bearers, developers and promoters of ORM throughout the Fleet, the IIS can easily assume the same position vis-à-vis IARM.

One of the key reasons ORM has been adopted throughout the Fleet is because senior decision makers have been convinced of its applicability and utility in preventing

mishaps. With its established credibility and reputation, NPS can have tremendous influence over those same decision makers DOD wide. NPS can leverage this advantage by offering a weeklong, executive level course to senior decision makers (O-5 and above, and GS equivalent) in information assurance and its importance to the DON mission. This course would introduce the basics of information assurance and the critical role decision makers play in managing the risks associated with our computer networks. It would have at its core the IAMR process. This course could use the same philosophical approach as the Aviation Safety School's six-day Aviation Safety Commander (ASC) course offered to unit Commanding Officers, Officers-in-Charge, and Safety Officers of major commands. An NPS executive level course can be instrumental in raising awareness of network security and IA issues and the concepts of IARM given our increased reliance on computer networks and the information it carries. It may also facilitate meeting Presidential Decision Directive 63 (PDD-63) requirements to improve the security capabilities of our nation's cyber-based critical infrastructure, and thus be applicable DOD wide.

ORM enjoys widespread implementation throughout the Fleet because each unit has a safety function that is well trained, and can facilitate its practical application at the unit level. To promote the practical implementation of IARM throughout the Fleet, the IIS can also offer a more in-depth course for senior IT support personnel and those individuals assigned with network security duties. This course could emulate the approach that the Aviation Safety School uses with its 28 instructional-day course for unit Aviation Safety Officers. This IT support personnel/information systems security officer (ISSO) course can be tailored to focus on officer IT specialist and enlisted IT

support corps. This advanced course can be divided into the following areas, much like the SANS Institute uses during its conferences:

- Fundamentals of Information Assurance
- Firewalls and Perimeter Protection
- Intrusion Detection Systems
- Incident Handling
- Current High-Threat Vulnerabilities and Cracker Exploits
- Effective Audit and Vulnerability Assessments
- IARM

The above two courses can be offered in cooperation with other DOD, government, academic or civilian institutions (e.g. SANS Institute, Carnegie Mellon, National Security Agency (NSA), Fleet Information Warfare Center (FIWC), etc.) and tailored to the needs of the participants if warranted. Classified portions of the above courses can also be offered as NPS has the required facilities to do this, and would make the executive level course more worthwhile for busy senior decision makers.

It is recognized that there are other entities endeavoring to accomplish these ends, but a more coordinated effort will gain efficiencies where none exist now. NPS is uniquely positioned to straddle the boundaries between the military, government, academia, and industry to realize these efficiencies. The NPS IIS can ultimately serve as the center for DON's efforts to improve IA throughout the Fleet and possibly throughout the Federal Government.

The Naval Postgraduate School (NPS) can test some of the concepts above by first introducing them into the Information Systems and Operations (ISO) curriculum. The purpose of the ISO curriculum is to "develop a cadre of Unrestricted Line (URL) Officers with the expertise to innovatively create concepts of war fighting and the application of information technology (IT) to implement them operationally." This cadre would benefit greatly form a thorough understanding of being able to apply the principles of ORM to IA (i.e., IARM) because they are the ones expected to facilitate the integration of IT into all the Navy does operationally.

The following is offered as a possible outline of IA curricula that can be applied to four targets groups: Line Officers, IT officer corps, enlisted IT support corps, and general users, and emulates closely the approach taken to implement ORM throughout the fleet. The note slides in appendix B is offered as the basis for an indoctrination presentation for IARM. [Appendix B and the note slides referred to were not included in this thesis. See Appendix B of LCDR Hernadez's thesis.]

A. INDOCTRINATION TRAINING OUTLINE

Audience: All Users

The purpose of this curriculum is to provide a basic understanding of what IA is, what risk management is, the benefits derived from it, the concepts that apply to it, and how to do time critical IARM. Content:

- IARM terms and definitions
- IARM introduction concept

- Four principles of IARM
- IARM vs. traditional approach
- Benefits of IARM
- Three levels of IARM
- Time critical IARM, examples and demonstration
- Specific applications (demonstrating applicability to existing IA processes and procedures)

Appendix B is offered as a possible presentation for this course. [Appendix B referred to was not included in this thesis. See Appendix B of LCDR Hernadez's thesis.]

B. USER OUTLINE

Audience: Junior IT Support Personnel

This curriculum is applicable to all users who use IT as a vital portion of their everyday duties, and the more junior members of the IT support corps referred to below, with the purpose of expanding their understanding of IA and the deliberate five-step process of IARM. Content: Indoctrination Training plus:

- Fundamentals of Information Assurance (IA)
- Deliberate IARM process and demonstration
- Basic vulnerability identification, tools, examples
- Vulnerability assessment tools and examples

- Risk assessment tools and examples
- Deliberate IARM practical exercise
- Specific applications (demonstrating applicability to existing IA processes and procedures)

C. INFORMATION TECHNOLOGY SUPPORT CORPS OUTLINE

Audience: Experienced IT Support Personnel and System Administrators

This curriculum is applicable to those more senior who actually maintain, support and administrate information systems within their commands with the purpose of expanding their understanding of current threats and vulnerabilities, and provide the tools necessary for implementing IARM in their command. Content: Users Curriculum plus:

- Advanced Information Assurance
- Firewalls and Perimeter Protection
- Intrusion Detection Systems
- Incident Handling
- Current High-Threat Vulnerabilities and Cracker Exploits
- Basics of effective Audit and Vulnerability Assessment
- In-depth vulnerability identification tools and examples
- Risk assessment tools and examples (cross section of available tools)
- Command implementation and leadership concepts

- Specific applications (demonstrating applicability to existing IA processes and procedures)

D. INFORMATION TECHNOLOGY (IT) OFFICER CORPS OUTLINE

Audience: IT Officer Specialist

This curriculum is applicable to those officers who are the enablers of the integration of IT into the everyday activities that are performed in the DON with the purpose to give enough knowledge to understand in-depth and deliberate IARM, what IARM can provide, and how to implement it within their units. Contents: IT Support Corps curriculum plus:

- Introduction to Information Operations (IO)/Information Warfare (IW)
- Advanced studies on the current threats and vulnerabilities
- Specific Applications

E. SENIOR LEADERSHIP OUTLINE

Audience: O-5 and Above (GS equivalent)

This curriculum is applicable to the senior leadership in the DON who will make IARM implementation effective through control of the rewards system used in the DON, with the purpose to provide a basic understanding of the IARM process, the benefits derived from it, the three levels and some of the applications of IARM. Content:

- IA background

- Current threats and recent exploitations (classified if necessary)
- Three levels of IARM
- Five step process of IARM
- IARM vs. traditional approach
- Specific fleet applications
- Benefits of IARM

APPENDIX D. OPERATIONAL RISK MANAGEMENT (ORM) OPNAV INSTRUCTION 3500.39A

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

and
HEADQUARTERS
UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

OPNAVINST 3500.39A
MCO 3500.27A
N09K
SD
26 SEP 00

OPNAV INSTRUCTION 3500.39A
MARINE CORPS ORDER 3500.27A

From: Chief of Naval Operations
Commandant of the Marine Corps
To: All Ships and Stations

Subj: OPERATIONAL RISK MANAGEMENT (ORM)

Ref: (a) DODINST 6055.1 (NOTAL)

Encl: (1) Introduction to Operational Risk Management

1. Purpose. To establish ORM, in accordance with reference (a), as an integral part of naval operations, training and planning at all levels in order to optimize operational capability, readiness, and enhance mission accomplishment.

2. Cancellation. OPNAVINST 3500.39 and MCO 3500.27.

3. Background

a. Uncertainty and risk are inherent in the nature of military action. The success of the Naval Services is based upon a willingness to balance risk with opportunity in taking the bold and decisive action necessary to triumph in battle. At the same time, commanders have a fundamental responsibility to safeguard highly valued personnel and material resources, and to accept only the minimal level of risk necessary to accomplish an assigned mission.

b. ORM is an effective process for maintaining readiness in peacetime and achieving success in combat without infringing upon the prerogatives of the commander. Historically, the greater percentage of losses during combat operations was due to

mishaps. Unnecessary losses either in battle or during training are detrimental to operational capability. Since 1991, ORM, applied both in day-to-day operations and during crisis periods, has produced dramatic results in reducing these losses. This instruction supports the guidance provided in reference (a) to integrate this effective technique throughout the Department of Defense. It provides a means to help define risk and control it where possible, thereby assisting the commander in choosing the best course of action and seizing the opportunities which lead to victory.

c. All naval missions, as well as daily routines, involve risk. Every operation, both on and off-duty, requires some degree of decision making that includes risk assessment and risk management. The naval vision is to develop an environment where every leader, Sailor, Marine and civilian is trained and motivated to personally manage risk in everything they do, both in peacetime and during conflict, thus successfully completing all operations with minimum risk.

3. Scope. This instruction applies to all Navy and Marine Corps activities, commands and personnel. Addressees should, as appropriate, issue an implementing instruction to augment this policy, including command-specific applications and requirements.

4. Discussion. ORM is a decision making process that enhances operational capability. Naval Warfare Publication 1 states, "Risk management and risk assessment are formal, essential tools of operational planning. Sound decision making requires the use of these tools both in battle and in training." ORM, described in enclosure (1), is a method for identifying hazards, assessing risks and implementing controls to reduce the risk associated with any operation. Implementation of ORM in the Department of the Navy will be accomplished as follows:

a. ORM will be included in the orientation and training of all military personnel. Level of training will be commensurate with rank, experience and leadership position.

(1) ORM training shall be incorporated into leadership courses, General Military Training and courses where operational employment, safety, or force protection are addressed (e.g., safety schools, initial warfare qualification schools, and tactical or operational level war fighting courses). ORM training shall be incorporated into existing training periods on safety and operational planning/decision making whenever possible.

(2) The ORM process and its specific application to pertinent subjects shall be integrated into fleet tactical training, Personnel Qualification Standards(PQS), Naval and Occupational Standards, Individual Training Standards and the Marine Corps Combat Readiness Evaluation System.

b. ORM lessons learned will be submitted to Chief of Naval Operations (N09K) and/or Commandant of the Marine Corps (SD) for inclusion in ORM data bases.

c. The ORM process shall be integrated into all levels of a command.

(1) Hazards shall be identified, risks assessed, and controls developed and implemented during the earliest possible planning stages. Operations shall be continuously monitored for effectiveness of controls and situational changes.

(2) Information available through existing safety, training and lessons learned data bases will be considered whenever practicable in making risk decisions.

5. Action. All Navy and Marine Corps activities shall apply the principles of ORM in planning, operations and training. The ORM process shall be applied to optimize operational capability and readiness. ORM decisions are made by the leader directly responsible for the mission. Prudence, experience, judgement, intuition and situational awareness are critical elements in making effective risk management decisions. When the leader responsible for executing the mission determines that the risk associated with that mission cannot be controlled at his/her level, or goes beyond the commander's stated intent, he/she shall elevate the decision to his/her chain of command.

a. Chief of Naval Operations (N09K) and Commandant of the Marine Corps (SD) shall provide policy sponsorship and service approval of Navy and Marine Corps ORM.

b. Chief of Naval Operations resource sponsors shall integrate ORM into existing training topics during review of courses under their cognizance.

c. Chief of Naval Operations (N09K) and Commandant of the Marine Corps (SD) shall serve as technical advisors on ORM curricula.

d. Navy Warfare Development Command shall address ORM concepts and applications in appropriate doctrinal publications.

e. Systems Commands shall provide information, data and technical support for the resolution of hazards under their cognizance.

f. Chief of Naval Education and Training (CNET) shall:

(1) Develop curricula for and incorporate appropriate ORM instructions at each level of formal leadership training, General Military Training (GMT) and all courses where safety or force protection is or should be appropriately addressed.

(2) Integrate specific applications of the Operational Risk Management process into PQS.

g. Commanding General, Marine Corps Combat Development Center shall:

(1) Develop curricula for and incorporate appropriate ORM instructions at each level of formal leadership training, GMT and all courses where safety or force protection is or should be appropriately addressed.

(2) Integrate specific applications of the Operational Risk Management process into Individual Training Standards and the Marine Corps Combat Readiness Evaluation System.

(3) Address ORM concepts and applications in appropriate doctrinal publications.

h. Commander, Naval Safety Center shall provide on request ORM excerpts from mishap and hazard reports and analysis of loss data.

i. Naval Manpower Analysis Center shall incorporate the ORM process into Naval Standards and, where specific applications warrant additional requirements, Occupational Standards.

j. Fleet Commanders in Chief (CINCs) and Commanders, Marine Forces (COMMARFORs) shall provide resources necessary to implement Operation Risk Management in accordance with this instruction.

k. Fleet, Type and Marine Expeditionary Force (MEF) Commanders shall:

(1) Incorporate the ORM process into operations, exercises and training.

(2) Address the ORM process in post exercise/operation reports.

l. Unit Commanders shall:

(1) Implement the ORM process within their commands. Examples include, but are not limited to:

(a) Providing training to Command personnel on enclosure (1).

(b) Incorporating identified hazards, risk assessments and controls into briefs, notices and written plans.

(c) Conducting a thorough risk assessment for all new or complex evolutions, defining acceptable risk and possible contingencies for the evolution.

(2) Address the ORM process in safety, training and lessons learned reports. Reports should comment on hazards, risk assessments and effectiveness of controls implemented.

(3) Inform the chain of command as to what hazards cannot be controlled or mitigated at their command level.

V. E. CLARK
Chief of Naval Operations

J. L. JONES, JR.
Commandant of the Marine Corps

Distribution:
SNDL Parts 1 and 2
MARCORPS PCN 10203352700

GLOSSARY OF TERMS

1. Assurance

Grounds for confidence that a system design meets its requirements, or that its implemented satisfies specifications, or that some specific property is satisfied (CIAO 185).

2. Duty

A major part of a job; a group of closely related tasks. A collection of duties makes up a job. A duty must be observable and measurable, occupies a major part of the work time, and occurs often in the work cycle (NAVEDTRA 130A p. 3-1-2).

3. Information Assurance (IA)

Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (CIAO 188).

4. Information Assurance Risk Management (IARM)

The process of dealing with risk to information and data that is inherently associated with information operations and information systems, which includes risk assessment, risk decision-making, and implementation of effective risk controls (Hernandez 37).

5. Information Security

Actions taken for the purpose of reducing system risk, specifically, reducing the probability that a threat will succeed in exploiting critical infrastructure vulnerabilities using electronic, RF, or computer-based means (CIAO 188).

6. Information Systems (IS)

The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information (CIAO 188).

7. Information System Security

The protection of ISs [information systems] against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. IS security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communications controls needed to provide an acceptable level of risk for the IS and for the data and information contained in the IS (Naval Information 56).

8. Information System Security Manager (ISSM)

Person responsible to the activity's DAA who develops, maintains, and directs the implementation of the INFOSEC program within the activity. The ISSM advises the CO on all INFOSEC matters, including identifying the need for additional INFOSEC staff. Serves as the Command's point of contact for all INFOSEC matters and implements the command's INFOSEC program. Previously the ADP Security Officer (Naval Information 56).

9. Information System Security Officer (ISSO)

Person responsible for ensuring that security is provided for and implemented throughout the life cycle of an information resource. Responsible for implementing system specific security policies in the operational environment. ISSO's are typically responsible for single-user computers (e.g., personal computers and workstations), multi-user computers or departmental Local Area Networks (LANs). The ISSO assists the ISSM in implementing the command's INFOSEC program for an assigned system or area of control. Previously the ADP Systems Security Officer (Naval Information 56).

10. Information Technology

The hardware and software that processes information, regardless of the technology involved, whether computers, telecommunications, or others (CIAO 188).

11. Job

Made up of duties and tasks (NAVEDTRA 130A p. 3-1-2)

12. Network

Information system implemented with a collection of interconnected nodes. (CIAO 189).

13. Probability

The likelihood that a vulnerability will result in data loss or compromise based on factors such as physical location, network services provided, network protocols, operating systems, personnel, and historical information. An expression of the possibility of a successful exploitation (Hernandez 36).

14. Risk

The probability that a particular critical infrastructure's vulnerability being exploited by a particular threat weighted by the impact of that exploitation (CIAO 190).

15. Risk Assessment

Produced from the combination of Threat and Vulnerability Assessments. Characterized by analyzing the probability of destruction or incapacitation resulting from a threat's exploitation of a critical infrastructure's vulnerabilities (CIAO 190).

16. Risk Management

Deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level. Characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned value (CIAO 190).

17. Severity

The worst, credible consequence that can occur as a result of a vulnerability. It is the potential degree of data or information loss or compromise (Hernandez 35).

18. Task

A major part of a duty; clusters of tasks make up a duty. A task must be observable and measurable and performed in a relatively short period of time. Each task is an independent part of the job, and is independent of other tasks (NAVEDTRA 130A p. 3-1-3).

19. Vulnerability

A characteristic of a critical infrastructure's design, implementation, or operation of that renders it susceptible to destruction or incapacitation by a threat (CIAO 191).

20. Vulnerability Assessment

Systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product to determine the adequacy of security measures, identify security deficiencies, evaluate security alternatives, and verify the adequacy of such measures after implementation (CIAO 191).

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"4-2 CG Resource Management.doc" www.swos.navy.smil.mil - /30Lessons/IOLC/Course Guide/ 10 October 2000. <http://www.swos.navy.smil.mil/30%20Lessons/IOLC/Course%20Guide/> (18 February 2002)

"About the CEE." Center for Executive Education. < http://www.cee.nps.navy.mil/>. (7 February 2002).

Bureau of Naval Personnel. Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards Volume I: Navy Enlisted Occupational Standards (NAVPERS 18068F) Milington: January 2002.

Bureau of Naval Personnel. Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards Volume II: Navy Enlisted Classifications (NECs) (NAVPERS 18068F) Milington: January 2002.

Bureau of Naval Personnel. Navy Officer Manpower and Personnel Classifications Volume 1: Major Code Structures. (NAVPERS 158391) Milington: October 2001.

Chief of Naval Operations (CNO) N6. Navy Information Assurance (IA) Program (OPNAVINST 5239.1B) Washington D.C.: 19 November, 1999.

Chief of Naval Operations (CNO) N643. Introduction to Information Assurance (IA) Publication (Module 5239-01) Washington D.C.: 15 May, 2000.

Denning, Dorothy E. *Information Warfare and Security*. Boston: ACM Press, 1999.

Hernandez, Ernest D. *Using Operational Risk Management (ORM) to Improve Computer Network Defense (CND) Performance in the Department of the Navy.* Thesis. Naval Postgraduate School, Monterey. March 2001.

"Information Systems Technician." Bureau of Personnel. <http://www.persnet.navy.mil/pers2/Hard%20/Cards/IT.doc>. (February 26, 2002).

"Information Systems Technician 'A' School." Information Systems Technician 'A' School: Phase I CD-ROM, Great Lakes: Service Schools Command, 2002.

Mayo, Richard W. to NAVADMIN. 2 August 2001. "Information Professional (IP) Community." Washington D.C. (RMSG 021133ZAUG01).

Mayo, Dick "Network Centric Warfare…It's Here," Presentation. Naval Postgraduate School, Monterey: 14 January 2002.

Merriam Webster's Collegiate Dictionary. 10th ed. Springfield: Merriam-Webster Inc., 1993.

"Mission." Space and Naval Warfare Systems Command. <http://enterprise.spawar.navy.mil/spawarpublicsite/>. (January 09, 2002)

"Mission, Vision And Guiding Principles." Fleet Information Warfare Center. <http://www.fiwc.navy.mil>. (09 Janaury 2002.)

Naval Education Training Command. Personal Performance Profile Based Curriculum Development Manual Volume I: Developers Guide (NAVEDTRA 131A) Washington D.C.: July 1997

Naval Education Training Command. Task Based Curriculum Development Manual Volume I: Developers Guide (NAVEDTRA 130A) Washington D.C.: July 1997

Naval Post Graduate School. Naval Post Graduate School Catalog: Academic Year 2001. Monterey:

"Nitras II Catalog Volume II CANTRAC Course Description DATA" Chief of Naval Education and Training. 17 February 2002. <https://pennnd09.cnet.navy.mil/cantrac/cantraccin.nsf/$$SiteOpen>. (17 February 2002)

"Other Programs" Center for Executive Education. <http://www.cee.nps.navy.mil/>. (7 February 2002)

"PMW-165 Home Page." PMW 165. <http://enterprise.spawar.navy.mil/spawarpublicsite/pd16/pmw165/index.htm> (9 January 2002).

Surface Warfare Officer School Command. "Manpower Documents: Lesson 4.9," Presentation. <http://www.swos.navy.smil.mil/Lessons/code20/dcore1.htm> (18 February 2002)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Department of the Navy
   Office of the Chief of Naval Operations (N6109)
   Washington DC

4. Fleet Information Warfare Center
   NAB Little Creek
   Norfolk, VA

5. Professor Rex Buddenberg
   Naval Post Graduate School
   Monterey, CA

6. LCDR Steven J. Iatrou
   Naval Postgraduate School
   Monterey, CA

7. Chair, IS Academic Group
   Naval Postgraduate School
   Monterey, CA