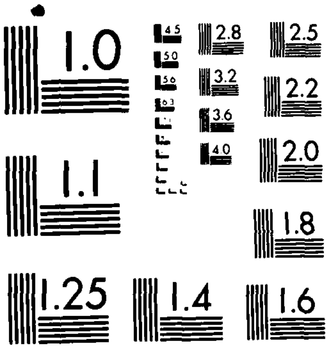
AD-A162 281   SECURITY REQUIREMENTS AND ORGANIZATION FOR NON-TACTICAL   1/1
ADP SYSTEMS ON SMALL SURFACE SHIPS(U) NAVAL
POSTGRADUATE SCHOOL MONTEREY CA J E ZAVODNY SEP 85

UNCLASSIFIED   F/G 9/2   NL


1.0
4.5
5.0
5.6
6.3
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.1
1.8
1.25
1.4
1.6

2

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

SECURITY REQUIREMENTS AND ORGANIZATION FOR NON-TACTICAL ADP SYSTEMS ON SMALL SURFACE SHIPS

by

Joseph E. Zavodny

September 1985

Thesis Advisor: Barry Frew

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER

2. GOVT ACCESSION NO. AD-A162 281

3. RECIPIENT'S CATALOG NUMBER

4. TITLE (and Subtitle)
Security Requirements and Organization
For Non-Tactical ADP Systems
On Small Surface Ships

5. TYPE OF REPORT & PERIOD COVERED
Master's Thesis
September 1985

6. PERFORMING ORG. REPORT NUMBER

7. AUTHOR(s)
Joseph E. Zavodny

8. CONTRACT OR GRANT NUMBER(s)

9. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Postgraduate School
Monterey, CA 93943-5100

10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS

11. CONTROLLING OFFICE NAME AND ADDRESS
Naval Postgraduate School
Monterey, CA 93943-5100

12. REPORT DATE
September 1985

13. NUMBER OF PAGES
66

14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)

15. SECURITY CLASS. (of this report)
UNCLASSIFIED

15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution is unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

small surface ships, non-tactical ADP systems, SNAP II, security requirements, security organization

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This thesis investigates the problem of non-tactical ADP system security requirements and security organizations on small surface vessels of the US Navy. It presents an overview of ADP security at the levels of the Federal government, Department of Defense, and Department of the Navy. The author researches the questions of whether there is a need for an abbreviated security manual for non-tactical ADP systems on small surface ships the level of detail required for such a manual, and the type of (Continued)

ABSTRACT (Continued)

security organization which might be required on a small surface ship. Conclusions are drawn which present the need for a security manual which pertains to specific ship types and classes, a possible outline for this security manual, and a possible shipboard security organization which is simple and effective.

✓

A-1

Approved for public release; distribution is unlimited.

Security Requirements and Organization
For Non-Tactical ADP Systems
On Small Surface Ships

by

Joseph E. Zavodny
Lieutenant, United States Navy
B.B.A., University of Notre Dame, 1978

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
September 1985

Author: Joseph E. Zavodny
Joseph E. Zavodny

Approved by: Barry Frew
Barry Frew, Thesis Advisor

Jack LaPatra
Jack LaPatra, Second Reader

for Willis R. Greer, Jr., Chairman,
Department of Administrative Sciences

K.T. Marshall
Kneale T. Marshall,
Dean of Information and Policy Sciences

ABSTRACT

This thesis investigates the problem of non-tactical ADP system security requirements and security organizations on small surface vessels of the US Navy. It presents an overview of ADP security at the levels of the Federal government, Department of Defense, and Department of the Navy. The author researches the questions of whether there is a need for an abbreviated security manual for non-tactical ADP systems on small surface ships, the level of detail required for such a manual, and the type of security organization which might be required on a small surface ship. Conclusions are drawn which present the need for a security manual which pertains to specific ship types and classes, a possible outline for this security manual, and a possible shipboard security organization which is simple and effective.

TABLE OF CONTENTS

LIST OF TABLES

I. INTRODUCTION

In this age of constantly expanding computer technology there is often a tendency to "go with the flow" just to maintain an even par with the new technology. As new developments are presented and new machines are constructed, it is often difficult to keep a proper perspective as to what use these new computers will be put to, and how they will be managed. But what happens after the right machine is selected and matched to a corresponding "right" job? Once the initial deficiencies are identified and corrected, and the system is performing as expected, do the systems managers amd operators sit back and relax, their jobs completed? Not if they are good at their job and concerned about the systems they are responsible for. A major problem facing them now is that of system security. They must now proceed with the security plans which were, hopefully, designed during the initial phases of the systems' development. The system must be protected from misuse, abuse, sabotage, theft, and a whole plethora of other security threats. This important issue is one which faces the managers of all types of ADP systems in both the civilian world and the military.

The military aspect of ADP security is one that is especially sensitive due to the nature of the military's purpose. The military makes use of many different types of computer systems which perform functions that range from the control of guided missiles to the control of inventory and personnel records. Basically, these ADP systems can be divided into two separate categories; tactical and non-tactical. Each category requires specific types of security for system protection.

The US Navy has not let itself fall behind in the business of ADP acquisition and use. It has developed or acquired systems to fit its own particular needs in both the tactical and non-tactical areas, though the tactical area is far ahead of the non-tactical area as evidenced below. This is due to the necessity of maintaining a modern and effective arsenal. However, the Navy is currently beginning to expend more money and effort in the area of non-tactical ADP systems. According to LCDR Mark T. Brown, there is a "computer gap" in the Navy which is "seen in the increasing divergence of capability between its tactical and non-tactical computer systems." [Ref. 1] He cites as an example of this the emergence of LAMPS III into the fleet, a highly technical new tactical system, while at the same time the Navy is using a 20 year-old UNIVAC 1500 system, a computer-card reading, batch-processing, non-tactical ADP system, on large ships for non-tactical applications [Ref. 1: p. 44]. Up to this time, the UNIVAC 1500 appeared to be the only large-scale non-tactical ADP application in the fleet. The SNAP I system (Shipboard Non-tactical ADP Program), the first part of a two-part program to modernize and expand the non-tactical automatic data processing capability of ships, was directed towards the replacement of UNIVAC 1500 computer systems aboard large ships [Ref. 2].

The second part of the program being introduced into the fleet at this time is the SNAP II system. It is currently installed (or being installed) in some 90 surface ships, with another 360 vessels slated to receive it in the future [Ref. 3]. On the deep-draft (large) ships SNAP I will be an update to already existing systems, but for the small ships SNAP II will b- a brand new automated system which will replace the outdated manual systems.

There is a need at this point to differentiate between the terms "large ship" and "small ship". A large ship is a deep-draft vessel, i.e., aircraft carriers, replenishment ships, amphibious ships, etc. Small ships are classified, for the purpose of this research, as cruisers, destroyers, frigates, mine countermeasures ships, research vessels, and salvage ships. It is the large ships which have, in the past, been the recipients of the non-tactical ADP systems mentioned above. Small ships have been forced to do without any kind of automated system for non-tactical ADP applications, save a system brought onboard by a resourceful crewmember. Size is not the only differentiating factor. Most large ships have an extensive command and control capability, thus giving them another reason for having the first shot at the initial installation of ADP equipment. In this thesis, the author will focus on the group of vessels classified as "small ships".

With the advent of SNAP II and other forms of non-tactical ADP systems in the fleet, there is an urgent need for some form of security program to protect these systems. This need is most pronounced in the small ships because they are new entries into the arena of automated data processing. That, and the fact that the author's professional background is in small surface ships, is the basis for the area of research that this thesis will encompass. Most instructions and directives in the Department of the Navy (DON) have, up to this time, focused primarily on the shore-based ADP system or the non-tactical ADP system on large ships. It is the contention of the author that there is a difference between the needs of a large ship/shore-based ADP system and the needs of the SNAP II-type system of a small ship in the areas of shipboard ADP security organization and shipboard ADP security requirements. The author also contends that there is a need for a separate security program which is suitable for small ships which excludes all of the extraneous requirements pertinent to large sytems.

In the course of this thesis the author will attempt to answer the following questions. First, is there a need for an abbreviated ADP security manual for small ships? If so, what level of detail is required, and what items will determine that level? Second, for an afloat unit, what sort of standard ADP security organization is required? Who should perform what functions, and why? Finally, how can these areas be addressed so that they can be of use to, and be made available to the fleet?

In order to arrive at the point where these questions can be answered, it is necessary to gain a basic understanding of ADP security. The author will begin with a basic overview of ADP security including its' theory, application to the public sector and Department of Defense (DOD) in general, and those requirements for security which are imposed by the Federal government and specifically the DOD. After an understanding of the basic tenets of ADP security has been established, the author will present an overview of current DON ADP security requirements and regulations, concentrating on directives, instructions and technology presently in effect. Once the foundations of ADP security requirements currently in effect have been presented, the author will present the unique requirements for ADP security on small shi¬s, followed by a discussion of what type of security organization fits them best. Finally, conclusions and recommendations will be offered.

II. OVERVIEW OF ADP SECURITY

A. DEFINITIONS

In order to better understand the ADP security problems facing a small ship it is necessary to first delineate exactly what ADP security is, what it entails, what forms of ADP security are currently available, and what basic requirements are imposed by the Federal government and the Department of Defense.

First, what exactly is ADP security? A good definition is found in FIPS Pub 102: "Computer security is the quality exhibited by a computer system that embodies its protection against internal failures, human errors, attacks, and natural catastrophes that might cause improper disclosure, modification, destruction, or denial of service." [Ref. 4] This definition is followed by an amplifying statement that the computer security of a system is a relative quality, not an absolute state to be achieved, and that security applies to both software and hardware. Another necessary definition is that of a security requirement; an identified computer security need [Ref. 4: p. 12]. The amplification statement is far more complex than the definition itself, but it is felt that it lends an expanded viewpoint to the definition:

> Computer security needs are derived from governmental policy, agency mission needs, and specific user needs.

> Governmental policy relating to computer security is expressed in laws and regulations; agency security needs are found in the agency's standards and policies; and user security needs originate in the application characteristics. Security requirements are expressed in increasing detail as one progresses from high-level general description of the system through lower levels of detailed specification. Security requirements need frequent review to insure their accuracy. [Ref. 4: p. 12]

B. FORMS OF ADP SECURITY

Now that the basic definitions of ADP security and security requirements have been explained, the author will present a brief overview of the different forms of ADP security which are in use today. Many of these will not be applicable to the requirements of a small ship, but they will help to provide a background as to how the various problems facing a small ship can be rectified.

The author has already established that, as automation increases and the reliance on computer/ADP systems grows, it becomes increasingly important to ensure that the information entrusted to these systems is protected [Ref. 5]. There are a large number of threats facing these ADP systems. These threats include unauthorized access by people to specific areas and equipment; ADP hardware failures; failure of supporting utilities; natural disasters; human errors; nonavailability of key personnel; neighboring hazards; tampering with input, programs or data files; and compromise of data through interception of acoustical or electromagnetic emanations from ADP hardware [Ref. 6]. Each threat has a specific way it can be countered, from bomb-proofing to internal protection of the programs.

Physical protection of the ADP equipment is usually the easiest to provide in for normal situations on land-based facilities. The problem becomes greater in the shipboard environment, as will be discussed in Chapter IV. In the civilian commercial environment it appears that the focus is on the techniques for information protection which range from simple procedural controls to complicated controls embedded within the hardware and software of the computer system itself, as opposed to the physical protection of the equipment [Ref. 5: p. 11].

Some examples of the internal security techniques in use today include the security kernel concept, information encryption (for communications security), inference controls for statistical data bases, a total distributed general purpose computing system that can enforce a multilevel security policy, and the development of technology for a computer system that can be trusted to enforce security on its own [Ref. 5: p. 11]. Of these techniques, the one of most importance to the topic of ADP security on small ships will be the security kernel concept, and it will be discussed more fully in a later chapter. The other techniques are geared towards larger, more complex systems and are mentioned only as examples of what techniques are currently available for use today.

C. ADP SECURITY REQUIREMENTS OF THE FEDERAL GOVERNMENT

As previously mentioned, there has been a proliferation of computer usage in the past years by the Federal government. This increased growth in usage has precipitated an increased need for adequate security. To provide guidelines and recommendations for these policies there are a vast number of publications, bulletins and instructions which have been issued on the subject of computer and ADP security. The majority of these publications come from the Department of Commerce's National Bureau of Standards and are published as Federal Information Processing Publications (FIPS Pubs). A sampling of those dealing with ADP security are listed in Table I. Though not all-inclusive, this listing gives a general idea as to the titles available, and also to the number of regulations which can be applicable to this subject.

For the Federai government, the general objectives of ADP security programs are

1. data integrity
2. data confidentiality
3. ADP availability

TABLE I

FIPS PUBLICATIONS

1. FIPS Pub 31: "Guidelines for ADP Security and Risk Management"
2. FIPS Pub 38: "Guidelines for Documentation of Computer Programs and Automated Data Systems"
3. FIPS Pub 39: "Glossary for Computer Systems Security"
4. FIPS Pub 41: "Computer Security Guidelines for Implementing the Privacy Act of 1974"
5. FIPS Pub 65: "Guideline for Automated Data Processing Risk Analysis"
6. FIPS Pub 73: "Guidelines for Security of Computer Applications"
7. FIPS Pub 74: "Guidelines for Implementing and Using the NBS Data Encryption Standard"
8. FIPS Pub 83: "Guideline on User Authentication Techniques for Computer Network Access Control"
9. FIPS Pub 88: "Guidline on Integrity Assurance and Control in Database Administration"
10. FIPS Pub 102: "Guideline for Computer Security Certification and Accreditation"

4. protection against accidental/deliberate acts [Ref. 7]

Dependent on the specific application of the ADP system is the method used to meet the above objectives and any specific objectives unique to the application. To achieve these objectives, basic controls are described. Selection of the controls that are applicable and necessary for a given application system depends both on its security objectives and on the environment in which the system operates. Some controls are implemented by hardware, the operating system or by the facility management [Ref. 7: p. 11]. These basic controls are:

1. data validation
2. user identity verification
3. authorization
4. journalling
5. variance detection
6. encryption [Ref. 7: pp.11-23]

Though identification of the basic controls listed above may appear simple, it is not. It is recommended that it be done on a continous basis throughout the application system life cycle, and changes made as necessary along the life cycle. Three phases of the life cycle are mentioned in the government publications; initiation, development, and operation [Ref. 7: p. 23]. Outlined are procedures which are recommended to be taken at each of these phases. These include: security feasibility studies and initial risk assessment in the initiation phase; security requirements definition, designs for security inherent to the system, security programming practices, and test and evaluation of security software in the development phase; and data control, employment practices, security training, security variance responses, software modification, hardware maintenance, and contingency planning in the operation phase [Ref. 7: pp. 23-43]. The publication goes into more specific detail than is necessary for the purposes of this thesis at this time. It is important to remember that though these procedures are listed within various phases, security planning and maintinance are ongoing occurrences, and steps must be planned in order to correct variances or problems as they arise.

In addition to the guidelines related above, there is also a security certification and accreditation program called for by the Federal government. This is detailed in FIPS Pub 102, and it carries further, the requirements listed for basic security. These rules form the basis for the regulations promulgated by all government agencies.

D. ADP SECURITY REQUIREMENTS OF THE DEPT. OF DEFENSE

Given that some of the pertinent sources of rules, regulations, and requirements for ADP security within the framework of the Federal government have been identified, it is now necessary to relate the posture of the Department of Defense (DOD) on ADP security. Understandably, there is a need for a higher degree of security awareness in the DOD as opposed to the majority of the Federal government, specifically in the areas of national defense. Therefore, it should follow that there is more emphasis placed on computer security in the DOD.

In order to determine the needs for computer security, the DOD is continuously conducting tests, research studies, and designing systems to alleviate the threats to its ADP and computing equipment. In 1981 the DOD Computer Security Evaluation Center (DODCSEC) was established to "complement the established responsibilities of DOD components relating to the overall policy, security evaluation, and approval of computer systems . . . ." [Ref. 8] This center was created to aid in accomplishing the primary goal of the DOD with regard to ADP security: to acquire a secure system,

> one which will control, through use of specific security features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information. [Ref. 9]

The main thrust of their work is to thwart the penetration of the computer systems by the use of a Trusted Computer System.

The Trusted Computer System (TCS) is a relatively new idea. It is a system that employs sufficient hardware and software integrity measures to allow its use for processing sensitive information [Ref. 8: p. 57], and, in order for a system to be trusted, the system must "reliably enforce a specified policy for accessing the data it processes while it accomplishes the functions for which it was built." [Ref. 10] In building this type of system, the designer must decide which security rules the system will enforce, and then be able to assure that the system enforces them. The principle recommendations to developers are that they consider the security requirements of each system as a part of its user-visible behavior, rather than as a separate set of requirements; continue to think about security throughout the design and implementation of the system; and use the best available software engineering technology [Ref. 10: p. 86].

The DODCSEC has developed criteria for evaluating the hardware/software systems used in processing classified information. The basis of this program is the Trusted Computing Base (TCB) which is the protection mechanisms of a system (hardware, firmware, and software) that are responsible for enforcing a security policy [Ref. 10: p. 89]. In this criteria are four hierarchical divisions, with D being the minimal, thru A for verified protection; and each division is broken up into numbered classes. The higher the class number, the greater the trust that can be placed in the system. These divisions are intended to represent major differences in the ability of the system to meet security requirements, while the classes represent incremental improvements [Ref. 10: p. 89]. These criteria are at present generally being used in the requirements phase of system development as a way of specifying security requirements that correspond to the needs of a system, in addition to their use in system evaluation.

The DOD is highly motivated in promoting the concept of the Trusted Computer System, and is gearing much of its computer research in that direction. There are a number of projects underway to develop trusted systems, including efforts to build trusted network interfaces [Ref. 10: p. 91].

Even though it appears that the Trusted Computer System is the way of the future for DOD ADP security plans, there are some opponents to this concept. The opposition is not towards the basic idea of computer security, but towards the path being investigated. It is noted that the vast majority of computer-related crimes have been committed by personnel who have authorized access to the resources they misused [Ref. 9: p. 61]. The opponents do not have an alternative plan to thwart this misuse by authorized users except to limit access to the system.

E. SUMMARY

Up to this point, the basic ideas of ADP security, Federal government ADP security sources and requirements, and the requirements and postures of the Department of

Defense on ADP security have been shown. This information is the foundation for the US Navy's requirements, goals, and policies on ADP security.

III. ADP SECURITY IN THE US NAVY

In this chapter the author will present an overview of the contents of OPNAVINST 5239.1A, DON Automatic Data Processing Security Program, dated 3 August 1982. This instruction forms the heart of ADP security in DON and an understanding of its contents is necessary for all personnel who have any contact with an ADP system. In order to present a more concise appearance and to make it easier for the reader to follow, all facts and references in this chapter are from OPNAVINST 5239.1A unless otherwise noted.

A. SCOPE AND OBJECTIVES

This instruction applies to all DON activities and DON-related contractors, and is intended to serve as a management tool which combines all necessary security requirements from higher concerns, and promulgates them in a simpler format. It covers the areas of policy, responsibility and procedures for the establishment and maintenance of ADP security programs, implementation guidance, and assistance and direction in developing and applying cost-effective security measures for the protection of DON ADP systems and stored and processed data.

The objectives of the instruction are to:

1. Provide centralized guidance and uniform policy

2. Provide a program which is responsive to the security requirements and needs of ADP systems
3. Provide for operational reliability and asset integrity
4. Provide realistic guidance and generalized procedures to ensure that all data are adequately protected against accidental or intentional destruction, modification, and disclosure, and users are protected against denial of service which may result from events such as fraud, misuse, espionage, sabotage, malicious acts, natural hazards, or fire.

In this instruction, various terms are used which may not be familiar to the reader. An ADP system is an assembly of computer equipment, facilities, personnel, software, and procedures configured for the purpose of classifying, sorting, calculating, computing, summarizing, storing, and retrieving data and information with a minimum of human intervention. There are three types of data levels mentioned throughout the instruction. Level I is classified data; Level II is unclassified data requiring special protection; and Level III is all other unclassified data.

It is an established fact that ADP security is an all-hands responsibility which encompasses the following elements: physical, administrative/operating procedures, personnel, communications, emanations, hardware, software, and data. Due to the high importance placed on ADP security, it is necessary that the program be carefully managed, regularly reviewed, continuously monitored, and routinely audited. For this to be accomplished, DON has established a thirteen-point ADP security policy. In brief, these points are:

1. A commanding officer and the ADP security staff will take the necessary steps to provide an adequate level of security for all ADP systems. They will implement the mandatory procedures for risk assessment, security test and evaluation (ST&E), and contingency planning.
2. Risk assessments will be an integral part of most ADP security decisions.
3. Technical assistance for risk assessments, ST&E, or a contingency test will be provided by Commander, Naval Data Automation Command.
4. When a peripheral or remote device is to be connected to an ADP system or network processing Level I or II data and will be used by personnel of an activity that is not responsible for the security of the host system, the security of the peripheral is the responsibility of the activity responsible for security of the host ADP system or network.

5. All DON ADP-related activities will comply with OPNAVINST 5239.1A.

6. OPNAVINST C5510.93D contains guidance for the policy on TEMPEST requirements.

7. All ADP activities will meet accreditation requirements as described below.

8. Activities processing Level I high security data are subject to additional requirements from outside the DON.

9. ADP security documentation disclosing vulnerabilities or exploitation techniques will be marked "For Official Use Only."

10. Software and files providing internal security controls, passwords, or audit trails for ADP systems will be safeguarded to prevent unauthorized modification.

11. Use of the Data Encryption Standard is prohibited for ADP systems processing Level I data.

12. Many products available commercially are not sanctioned for use by DON activities. Plans implementing these technologies for Level I data processing should include ascertaining if these products are to be endorsed for DON use. Requests for information should be forwarded to COMNAVDAC.

13. All ADP activities which process data covered under other instructions will comply with the more stringent requirements.

In addition to the above listed policies, each commanding officer is responsible for the security of the ADP system under his command and must meet additional requirements which include development of an Activity ADP Security Plan (AADPSP), appointment of an ADP Security Officer (ADPSO), and ensure that proper care is taken to ensure the security of his installation.

In the area of ADP security, an ADP activity or network is either accredited or not accredited. Accreditation describes the process whereby information pertaining to the security of an ADP activity or network is collected, analyzed, and submitted for approval to the appropriate Designated Approving Activity (DAA). After a review of this material, the DAA will either concur, thereby indicating that a satisfactory level of operational security is present; or not concur, indicating that the level of risk either has not been adequately defined or has not been reduced to an acceptable level for operational requirements. If not accredited, an activity may be issued an interim authority to operate, contingent upon improved security within a set periond of time. Accreditation responsibilities differ for the various levels of data (Levels I, II, III).

Office Information Systems (OIS) are applications of automated technology for document preparation, storage, retrieval, manipulation, and distribution in an office environment. Office Information System Equipment (OISE) differs from ADP equipment, in that, OISE is primarily limited to document text preparation and handling applications, whereas ADP equipment is designed to process a variety of applications developed using a general purpose data processing language. There are specific security requirements relative to an OIS. Due to the limited scope of OIS applications, adequate security countermeasures can be identified and implemented with less procedural effort than would be required for a comparable ADP system. The minimum security requirements for an OIS include; operational reliability and asset integrity for prevention of loss from natural hazards, fire, theft, and malicious acts. The OIS is a system comparable to the non-tactical ADP systems found on small ships (i.e., SNAP II), and will be discussed in more detail in a later chapter.

B. RISK MANAGEMENT

Risk management is the determination of how much protection is required for an ADP system and how much protection already exists. It is an ongoing effort, and risk must be re-evaluated whenever changes occur to the ADP environment. The risk management program consists of three phases:

1. Development of an Activity ADP Security Plan
2. Risk assesment
3. Countermeasure implementation and effectiveness review.

The AADPSP implements the security policies set forth in OPNAVINST 5239.1A. It establishes local security policies, defines security scope and objectives, assigns responsibilities, sets short/long-range security goals, and addresses security for all aspects of the local ADP elements. It is an important document which must be utilized for the management of the ADP security environment.

Risk assessment consists of two distinct parts; threat and vulnerability identification, and countermeasure identification. A threat is defined as any agent capable of reducing the effectiveness of an ADP activity or network, thereby degrading mission accomplishment. A vulnerability is a weakness that may be exploited by a threat agent to cause harm to the ADP activity or network. Countermeasure identification is the process of determining the most cost-effective method of countering a threat or vulnerability.

There is a specific risk assessment strategy laid out in the instruction. The first step is to conduct an ADP Security Survey which will provide basic information about the ADP security environment and help determine the scope of the risk assessment effort. Once this has been accomplished, the DAA will determine the risk assessment methodology to be used. There are two methods available, and the complexity of the ADP environment is the determining factor as to which one will be used. The environment complexity is governed by the level of data processed, security mode of operation, ADP system configurations and locations, and the criticality of the mission. Method I is the standard method for use in most ADP environments; Method II is for use in less complex ADP environments. Method I provides for greater detail than Method II, and Method II does not provide for the interaction of threats and evaluation of threats by impact areas. There are other methods available, but permission must be obtained from CNO for their use. The basic steps for both methods are:

1. Asset identification and valuation
2. Threat and vulnerability evaluation
3. Assessment of the frequency of successful attack
4. Computation of the Annual Loss Expectancy (ALE)
5. Selection af additional countermeasures based on return on investment and reduction of the ALE.

Once the risk assessment has been completed, countermeasures must be selected which will make the level of risk acceptable. There are seven groupings of countermeasures based on correcting weaknesses in the ADP environment. Each method within the groupings is described in terms of:

1. Vulnerability--description of the weakness that could be exploited.
2. Countermeasure--description of an action, device, procedure, technique, or other measure that reduces the identified vulnerability.
3. Confidence--a judgement as to the effectiveness of an implemented countermeasure.
4. Cost factor--qualitative statement on the anticipated expense of implementing a proposed countermeasure. The actual costs should be determined by consulting the local procurement authorities.
5. Caveats--limitations, unusual risks, dependencies, and/or disadvantages related to the proposed countermeasure.

By groupings, listed below are the various countermeasure techniques listed in OPNAVINST 5239.1A. The instruction states that the list is non-inclusive, but only contains the most common techniques.

1. Software countermeasures: security audit trails, threat monitoring, residue control, log-on attempts, unique password/authentication processes, password protection from visual observation, file encryption, data base protection, periodic inspections of hardware, controlling use of assembler language coding,

two-person control, periods processing, testing and debugging, security editing and accounting, software engineering tools, virtual machine monitors, password file encryption, secure subsystems, and security kernels.

2. Hardware countermeasures: protection-state variables, memory protection mechanisms, front-end machines, data base machines, tampering detection, and interruption resistant power.
3. Administrative countermeasures: security officer procedures, software development procedures, software maintenance procedures, batch input/output procedures, access procedures, waste procedures, emergency procedures, and operating procedures.
4. Personnel countermeasures: personnel control and compromise.
5. Emanations: emanation security.
6. Physical countermeasures: access to the computer center, physical layout, fire protection, environmental control system, and building construction.
7. Communications countermeasures: communications lines and links, terminal identification, handshaking, telephone instruments, protected distribution system and communications path alternatives.

The final step in the risk management program is countermeasure implementation and effectiveness review. This is done over a period of time. As the system changes and new threats are perceived, new countermeasures may be added as needed. The entire thrust of the preceding process is to gain a security accreditation and provide the best possible security for the system.

C. SECURITY TEST AND EVALUATION

Security Test and Evaluation is another part of the accreditation process. The primary purpose is to obtain technical information to support the DAA's decision to accredit an ADP activity or necwork. It consists of two interrelated phases. The first determines whether the necessary countermeasures have been installed, and the second determines whether the installed countermeasures are working effectively.

The resources expended and the level of detail required will depend upon the level of data being processed and the mode of operation. The results of the risk assessment will determine the level of detail and scope required. When the Commanding Officer is the DAA, the ST & E are the responsibility of the activity; otherwise it is performed by COMNAVDAC. Qualified personnel at the activity will perform the various steps of reviewing the risk assessment, developing the ST & E plan, executing the plan, and documenting the results.

D. CONTINGENCY PLANNING

The Contingency Plan is an important part of an ADP security program. DON activities dependent upon ADP to support mission accomplishment are required to develop a plan which would allow continuity of mission accomplishment during abnormal operating conditions. The contingency plan will consist of two distinct phases; the preparation phase and the action phase. The scope of the plan will be such that it identifies: actions required if the normal ADP environment is impaired or disrupted; actions required if the functional application or user is denied information or service; and actions required if the ADP activity suddenly had to expand processing capability to accommodate a national emergency or some other critical event.

Preparation of the contingency plan entails an in-depth look at emergency response, backup operations, recovery expectations, and an assessment of the necessity for emergency destruction of classified material. Once the plan has been completed, it is to be tested annually, and improvements made where necessary. No contingency plan is required if unplanned disruption of services would not have a critical impact on mission accomplishment; the DAA must be informed if this is the case.

E. ADDITIONAL INFORMATION

The remainder of OPNAVINST 5239.1A is comprised of various appendixes which offer a glossary of terms and definitions, samples of ADP security training plans, threat and vulnerability assessment worksheets, guidelines for ADP security documentation, DON security and audit controls, and mandatory minimum requirements for ADP activities including environmental and physical security, communications security, emanations security, and hardware/software security features.

F. CONCLUSIONS

As can be seen, the DON ADP security program is an extensive one which attempts to cover all aspects of the ADP security environment. But is it too extensive, too all-inclusive? Are there too many requirements and regulations which are mandatory but cannot be adhered to by the ADP organization of a small ship? These questions will be explored in the remaining chapters.

IV. SECURITY REQUIREMENTS FOR SHIPBOARD ADP SYSTEMS

A. INTRODUCTION

In the previous chapters the author has discussed the background of ADP security in terms of what it is, why it exists, the aspects of security and how they are interpreted by the Federal government, Department of Defense, and Department of the Navy, and the various requirements imposed on ADP systems by the agencies listed above. However, most of those requirements were devised with large ADP systems in mind. Because of this, and with the advent of non-tactical ADP systems being installed on small surface ships, it has been theorized that the current ADP security requirements in effect may be too extensive for these smaller shipboard systems. In this chapter the author will explore the unique security requirements for non-tactical ADP systems on small surface ships and some of the possible countermeasures available to combat perceived threats. The author will also address the subject of which sections of OPNAVINST 5239.1A have little or no relevence to non-tactical ADP security on small surface ships and how these sections can be adapted or removed.

B. NON-TACTICAL ADP SYSTEMS IN SMALL SHIPS

Small surface ships are beginning to acquire non-tactical ADP systems in the form of the SNAP II systems. Prior to the installation of these systems onboard, most small ships had to rely on the manual method of accomplishing any data processing tasks. The objective of SNAP II is to reduce the administrative burden on the fleet by eliminating much of the manual paperwork requirements in the forms of records and reports, and by reducing error rates and associated time by screen-correcting documents through on-line/immediate validation [Ref. 3: p. 20]. Presently there are four subsystems in SNAP II. They are:

1. System Management Subsystem (SMS). This performs system management and system service tasks in support of the other three subsystems.
2. Maintenance Data Subsystem (MDS). This system will support the ship's maintenance plan, including ship's force work list, maintain maintenance logs and files, automatically prepare OPNAV forms 4790/2K and 4790/CK, interface between maintenance and supply, and allow maintenance completion with needed supply items in a simpler manner than is presently being done.
3. Supply and Financial Management Subsystem (SFM). This system automates current supply procedures,

including inventory control, OPTAR accounting, and financial accounting.

4. Administrative Data Management Subsystem (ADM). This will provide support for those functions specifically related to shipboard administration. [Ref. 3: pp. 20-21]

As is readily apparent, SNAP II, when used properly, will be a boon to the surface fleet. Once this system is outfitted on board a small surface ship, what type of security threats exist, and what sort of security protection is required?

C. THREATS TO NON-TACTICAL ADP SECURITY IN THE SHIPBOARD ENVIRONMENT

It is quite easily understood that the environment on a naval vessel is fairly hostile to any type of system installed on board. In this section the author will identify those threats and vulnerabilities which relate to the non-tactical ADP system in the shipboard environment. This will not be an attempt to conduct a risk assessment, but only to provide the information necessary to identify the needs for ADP security, thus delineating shipboard security requirements.

Previously mentioned in Chapter II was a list of the possible types of threats which face ADP systems. The first of these threats was unauthorized access by people to specific areas and equipment. In the small ship environment this threat is not very prevalent. Most work areas where the non-tactical ADP system equipment would be used are small, and access to them will be very limited. In addition, when spaces on a vessel are not manned they are, as a matter of routine, locked. This, in addition to the possible use of an access list, would assist in deterring unauthorized access to the system equipment. The major threat in the way of unauthorized access would be the possibility of somebody being able to log onto the system without having the proper authorization allowing them to log on. One way to prevent this unauthorized usage and prevent tampering with input, programs, or data files is by the implementation of the security kernel concept.

The security kernel is a technology which provides a conceptual base on which to build a secure computer system using a methodical design process [Ref. 11]. It is a system beginning to see wide development in the commercial market. An example of this form of application is Honeywell's SCOMP, an implementation of a hardware/software general purpose operating system based on the security kernel concept [Ref. 12]. Though SCOMP is used in a large system, there are also applications being developed for the use of the security kernel in small systems. Research conducted at the Naval Postgraduate School concentrated on the applications of the security kernel for a multiprocessor microcomputer [Ref. 13]. It is this area of research which appears to be the possible solution to the access threat posed in the preceeding paragraph.

The security kernel approach is based on the concept of the reference monitor, which provides an underlying security theory for conceptualizing the idea of protection. In this way all active entities make referenc s to passive entities using a set of current access authorization. The security kernel consists of both hardware and software [Ref. 11: p. 14]. The purpose here is not to provide a detailed analysis of the security kernel, but to give a brief outline so that the concept can be understood and possibly applied to the problem at hand. In order for the security kernel to be properly developed, a specific security policy must be delineated. There are two types of policies for this system: nondiscretionary, which contains mandatory security rules that are imposed on all users; and discretionary, which contains security rules that can be specified at the option of each user. Both policies are addressed by the rules of the security model [Ref. 11: p. 15]. These policies should be determined on a class-wide basis for small surface ships, and possibly implemented as such.

In the security model, each subject and object of the reference monitor is given a security identifier termed an access class, which are compared at each state transition to determine whether a subject is allowed to access an object. By proper organization of a mathematical structure called a lattice, a wide range of policies can be supported [Ref. 11: p. 16]. The final basic premises of this concept are the two fundamental rules of the nondiscretionary policy; the simple security condition, and the "star" property. The simple security condition prohibits users from directly viewing data they are not entitled to see, and the "star" property helps to prevent all illicit indirect viewing of objects [Ref. 11: p.16]. On the negative side of the security kernel is the fact that if applied to inappropriate hardware, the security kernel can impose significant performance burdens [Ref. 10: p.94]. This problem can be eradicated by simply chosing the correct hardware as needed to ensure proper utilization of the kernel.

In the multiprocessor environment, the security kernel provides the mechanism for support of the security policy of the command. It is the author's belief that the proper implementation of a security kernel will provide a great deal of security for the system in the area of personnel trying to gain unauthorized access to the system.

A second area of threat is that of ADP hardware failure. This is very realistic in the small surface ship environment. Because of the nature of a small surface ship, there are many outside agents which can contribute to the failure of non-tactical ADP hardware. These include salt contamination of components, intense movement of the platform due to rough seas, and missile hazards, also due to rough seas. In addition there is also the possibility of failure due to a mechanical problem within the system itself. The particular hazards encountered due to the ship being at sea can be easily countered by standards being established for the equipment to negate the pitch and roll of the ship, much in the same way as current equipment onboard is protected. Missile hazard damage is minimized by a careful inspection of the space prior to going to sea. This is a normal procedure on all ships prior to getting underway. Salt contamination prevention is a function of where the equipment is placed, and the adequacy of the compartment 's water-tight integrity. In essence, the best protection against hardware failure is to ensure that the equipment is sturdy, and that the space housing it is properly secured.

Failure of supporting utilities can be a major problem on small surface ships, and it is not something that can be easily controlled. Power failures and air-conditioning losses are notorious common occurences on small surface ships. Power failures range from complete loss to improper voltage supplies. Electrical protection devices are necessary to prevent damage by a short-lived abrupt loss of power and voltage fluctuations. Unfortuneately, there is no real protection from a major power loss. Backup generators for a non-tactical ADP system are not feasible due to space and operational considerations. In fact, even tactical abilities are lost during a major power loss because all emergency power is shunted to the engineering plant (save emergency lighting and power for a small radio) in order to give the engineering personnel the ability to restore power. A battery pack with a duration of not less than one hour was recommended in order to protect memory during an unexpected loss of power refprd 14 Loss of air-conditioning to a space, necessary to keep the machinery cool, is another often-encountered problem. The only real effective measures for this type of problem would be to either minimize system usage, or shut it down entirely. Air conditioning loss for a short period of time will probably have little effect on the system equipment due to it's low power usage.

There are a number of natural disasters which can pose serious threats in the small surface ship environment. These include fire, flooding, and hurricanes. Not only do these pose a serious threat to the non-tactical ADP equipment, but also to the safety of the ship itself. Because of the consequences of fire and flooding to a small surface ship at sea, there are well-planned procedures to combat either of the two when they occur. These procedures usually concentrate more on relieving the threat quickly to prevent it from spreading than to the actual protection of the concerned equipment. This could have an adverse effect on the non-tactical ADP system that might get caught in a fire or flood, but unfortunately there are few other alternatives.

Human errors are basically a function of the amount of training given an individual prior to allowing them to use the system. Some of the possible errors can be quite cataclysmic. For officer personnel, the proper use of the SNAP II system is being incorporated into the curriculum at the Surface Warfare Officer School Command (SWOSCOLCOM) in the Basic Course, Department Head Course, PXO, and PCO courses. The level of instruction in each curriculum is to be geared towards the use of the system by the individual. Current plans are to provide training which will encompass all possible uses of the system [Ref. 3: p.21]. Training of this sort will not only reduce the possibility of human errors, but will also allow the system to be used to its full potential. At this time there is no equivalent course for enlisted personnel. There are a number of viable alternatives for training of enlisted personnel. When the SNAP II system was first readied for introduction to the fleet, it was recommended that training for enlisted personnel be conducted at organic training courses (PN, SK, YN schools, 3M school, etc) for those who will be operating the SNAP II system [Ref. 15]. Though being done on a minimal scale, there is another alternative, that of conducting the training at Fleet Training Centers. A major drawback for this alternative would be the extra funds required to implement the new courses. Funding is minimal for the first alternative. The author would recommend that training be continued in the source schools, but that some other sort of short course be implemented at the Fleet Training Centers for those not eligible for those schools.

The most devasting threat which faces the non-tactical ADP system of a small surface ship is that of battle-inflicted damage. Granted that this is the ultimate which can occur, and it is not a threat to the security of the system that can be easily defended against. But the threat does exist, and must be addressed. Unfortunately, the best defense is to not receive any battle damage. Damage as a result of battle that can be inflicted to the non-tactical ADP system is fire, flooding, or total destruction. Countermeasures for fire and flooding are already in ship's instructions, and there are no real countermeasures for total destruction.

As the author has related in the preceeding paragraphs, there are a number of threats which face the non-tactical

ADP system of a small surface ship, and some of them are unique to only this type of environment. Some of the threats have existing countermeasures which require little or no modification, whereas other measures must be implemented in their entirety. Now that the possible threats which exist have been identified, it will be easier to discuss the security requirements which are necessary for the non-tactical ADP system of a small surface ship.

D. SECURITY REQUIREMENTS

The author, in Chapter II, defined a security requirement as an identified computer security need. In this chapter the threats which face the non-tactical ADP system on a small surface ship have been discussed, along with some possible countermeasures for these threats. In this section the author will postulate what he believes to be the necessary security requirements, in terms of the security program in OPNAVINST 5239.1A, for a small surface ship.

Due to the uniqueness of small ships and the extent of the security necessary for a non-tactical ADP system, it is possible that the present security requirements in OPNAVINST 5239.1A are far too extensive for these types of ships. What is necessary is an instruction which contains the basic requirements for security and allows specific information to be added to it as appendices for the different classes of small surface ships, much on the same order as the format of the COMNAVSURFLANT Master Training Plan. As an example, it would be tailored for FFG-7 frigates by adding a FFG-7 appendix to the basic instruction. An instruction of this type would be far easier to use, and would undoubtedly provide a far more productive security plan.

There are some necessary sections which should be included in this generic instruction. These sections will follow the guide of OPNAVINST 5239.1A, but be pertinent to small surface ships only. As in all Navy instructions, the first section should define the scope of the non-tactical ADP security program as it relates to small surface ships. The second chapter should deal with the security organization, both of the the DON and the ship, outlining which officers are responsible for specific aspects of the system's security. This section will be further discussed in the course of Chapter V. Their duties and responsibilities should be made stringently clear, and easily understandable.

A section on accreditation is necessary also. For the case of small surface ships, the final accreditation authority should be the Type Commander (SURFLANT, SURFPAC). The author believes that by having the authority for accreditation at the Type Commander level it will enable ships to receive aid far easier in case the ship is having problems meeting requirements. It is expected that there will be only a limited amount of Level II data being used on these non-tactical ADP systems, with the majority of the information processed, being Level III. Because of this, the accreditation problem becomes much simpler. Security requirements for Level II data can be determined by the Commanding Officer and ADPSO, with any strengthening of the requirements left to the discretion of higher level commands [Ref. 16]. By having the instruction promulgated at the Type Commander level, specifically for small ships, it will provide a more standard level of security, thereby making it easier to enforce and maintain.

Requirements for accreditation should include a Method II risk assessment, development of an AADPSP, development of a contingency plan, and meet the minimum mandatory requirements for environmental and physical security. It is believed that the above requirements will be sufficient to guarantee the security necessary for the system. The author chose a Method II risk assessment because it is the proper one for a less complex ADP environment, of which the non-tactical ADP system is an example [Ref. 16: p. E-13]. Continuing with the theory of class-wide security instructions, a risk assessment can be made easier than would normally be expected. Since all ships of a class are similar, it follows that the assets, threats, vulnerabilities and countermeasures would also be similar. Generic risk assessment formats would be promulgated by the Type Commanders and used by the individual commands who would make necessary changes due to unique ship alterations, etc. Contingency plans and security plans will be developed in the same manner.

Included in this instruction would also be requirements for command review of the security program, to be conducted at intervals in compliance with current directives, which call for a review every three years or as necessary due to changes in the non-tactical ADP environment [Ref. 16: p. 8-1].

A training plan for non-tactical ADP security is a necessary part of this instruction. Improper training of personnel is as great a danger to the system as any other threat. All personnel using the system should be required to have adequate instruction prior to using the system. A Personnel Qualification Standard (PQS) developed for users would be an ideal method of training. As already stated, officers are to receive training at SWOSCOLCOM. A shipboard program should be outlined, and strictly enforced. The areas of knowledge required by OPNAVINST 5239.1A should be adhered to in this program [Ref. 16: p. 10-2].

Appendix J of OPNAVINST 5239.1A contains a listing of mandatory minimum security requirements. The requirements listed for environmental and physical security are very similar to requirements already enforced on small surface ships. For the purposes of this new instruction they should be tailored specifically for small surface ships so that there are no discrepancies. Examples include the requirement to keep all carpeted areas vacuumed frequently, and a section of mandatory requirements for activities processing Levels I and II data [Ref. 16: p. J-2]. These conditions do not exist on small surface ships.

As can be seen, the outline presented above is an alternative instruction to OPNAVINST 5239.1A for a small surface ship. This type of instruction would be much easier for the shipboard ADP security manager to follow in implementing a proper security program for his equipment. By not having to wade through a great amount of material not pertinent to his system, he will find that he has little problem making the security program work. Another positive outcome of this type of instruction would be a certain uniformity throughout the Surface Warfare community in the area of non-tactical ADP system security.

V. NON-TACTICAL ADP SYSTEM SECURITY ORGANIZATION

The mere presence of a non-tactical ADP security program does not guarantee that a system will be secure. There is also a need for a security staff to oversee the program to ensure its proper operation and maintenance. This chapter will discuss the present requirements for an ADP security organization, and the organization which the author believes would be more suitable for the non-tactical ADP system of a small surface ship.

A. PRESENT ADP SECURITY ORGANIZATION REQUIREMENTS

OPNAVINST 5239.1A delineates a specific ADP security organization for activities with ADP systems [Ref. 16: p. 2-5]. As in all Navy commands, the Commanding Officer has full responsibility for the security of the systems under him. He is responsible for ensuring the development of an AADPSP, appointing an ADPSO/OISSO, and ensuring that all other requirements of security are met.

Under the Commanding Officer, the ADP Security Staff is headed by the ADP Security Officer (ADPSO). He is responsible to the Commanding Officer for ensuring that all aspects of security are carried out. He must appoint the Network Security Officer (NSO) if needed, coordinate ADP security with the activity security manager, ensure that the

AADPSP is developed and maintained, appoint an ADP System Security Officer (ADPSSO) if needed, appoint a Terminal Area Security Officer (TASO) if needed, implement the Risk Management Program, carry out accreditation procedures, ensure development of contingency plans, assist the ADP security staff, ensure personnel security procedures are established, conduct systems tests and evaluations, develop a Risk Assessment Team Charter when required, and assume the ADP security staff responsibilities for any staff member not appointed. [Ref. 16: p. 2-9]

The Network Security Officer (NSO) is responsible for developing the standard security procedures governing network operations and ensuring that all required network countermeasures are utilized [Ref. 16: p. 2-11]. The ADP System Security Officer (ADPSSO) is appointed at the discretion of the Commanding Officer for each ADP system which processes or will process Level I or II data. This officer performs much the same duties as the ADPSO, but for his assigned systems. In addition, he must be the focal point for all security matters for the ADP systems assigned, execute the ADPSP, maintain an inventory of all ADP hardware, implemented system software releases, monitor system activity, maintain liason with remote facilities served by the ADP system, conduct risk assessment, implement appropriate countermeasures, and perform other tasks as indicated by the ADPSO [Ref. 16: p. 2-11]. The Terminal Area Security Officer (TASO) is appointed for remote facilities and enforces all security requirements implemented by the ADPSSO for remote terminal areas and is responsible for ensuring that proper countermeasures are in place [Ref. 16: p. 2-12].

The final member of the ADP Security Staff is the Office Information Systems Security Officer (OISSO). As OISs are considered a subset of an ADP system, the ADPSO is responsible for the security of the OIS. However, at activities which have only OISs, an OISSO will be appointed in place of an ADPSO and will assume those duties of an ADPSO which are applicable to OISs [Ref. 16: p. 4-1]. He will maintain an inventory of the OIS, ensure that OIS Security Operating Procedures are available, and be responsible for instructing users as to knowledge of OIS technology, OIS security, and OIS operations [Ref. 16: p. 4-4].

B. RECOMMENDED NON-TACTICAL ADP SYSTEM SECURITY ORGANIZATION

As can be seen above, the structure and responsiblities of the ADP Security Staff are complicated and immense. In most large activities, there are enough personnel to handle this additional workload. This is not the case on small surface ships. The wardroom (officer's complement) of a small surface ship is small--usually no more than 30 officers on the largest ships--and most have primary responsibilities which demand their full-time attention. In addition, most are required to perform collateral duties which take up their remaining time. No matter how important ADP security is, the job of ADP security officer will fall into this latter category.

The author believes that there is not a need for all of the positions required by OPNAVINST 5239.1A. First, there are not enough personnel on board a small surface ship to effectively man the positions adequately, and second, the non-tactical ADP system is not extensive enough to warrant it. The author suggests that the positions necessary to facilitate an adequate security organization of a small surface ship are the ADPSO and ADPSSO.

The ADPSO will perform those duties outlined in OPNAVINST 5239.1A, for his position, which are pertinent to a small surface ship's non-tactical ADP system. He will have overall responsibility for ensuring the security of the system and will report directly to the Commanding Officer in matters relating to security. The ADPSO position will be filled by a department head with this position being a collateral duty. The best possible choice would be the Operations Officer because his primary job already entails other points of security, and he would have less conflicts with the performance of his primary duties. The other departments heads, engineer and weapons, have responsibilities which do not allow the freedom that the operations officer enjoys. The chief engineer very rarely has time to get away from the engineering plant, and the weapons officer is usually concerned with nuclear weapons security, when applicable.

An ADPSSO is necessary to assist the ADPSO. No matter how small the system the author is convinced that ADP security is too important to leave to one person. The ADPSSO will perform the duties of his position as outlined in OPNAVINST 5239.1A that are pertinent to small surface ship systems. He will be responsible for the execution of the ADP security program. This position is best filled, again as a collateral duty, by a junior officer. It is difficult to ascertain from which department this officer should be, but it is definitely recommended that this duty be this officer's primary collateral duty. As already iterated, ADP security is the most important aspect of the ADP system to the ADP security staff, and the ADPSSO must be able to devote the necessary time to the proper performance of his job.

The author sees no need for the designation of a TASO, NSO, or OISSO in the small surface ship situation. Their duties as outlined, will fall within the purview of the

ADPSO and ADPSSO. In addition, the size of the non-tactical ADP system does not call for these extra personnel. If there are too many members of the security organization, it is quite possible that they will begin to work at cross-purposes.

There is a definite need for a training program to be established for the ADPSO and ADPSSO to be completed prior to assumption of their duties. It would be detrimental to the security of the system, due to the intricacies of ADP security, to place officers in those positions without the proper training. The most likely choice for coordinator of the training program would again be the Type Commanders, once they have established the various security manuals for the different classes of ships.

VI. CONCLUSIONS

In this thesis the author attempts to answer a number of specific questions. First, is there a need for an abbreviated ADP Security Manual for small surface ships, and if so, what is the level of detail required, and what items will determine that level? Second, what sort of ADP security organization is required for a small surface ship, who should perform what specific functions, and why? And finally, how can these areas be addressed so that they can be of use to, and be made available to the applicable portions of the fleet? Based on the material presented in the preceding chapters, the following conclusions can be drawn.

There is a need for an abbreviated ADP security manual for the non-tactical ADP systems of small surface ships. OPNAVINST 5239.1A is far too awkward and contains many extraneous parts to be used in this particular environment. It contains parts which do not pertain to the problems discussed for small surface ships, and it can be very confusing to try and elicit the sections pertaining to small surface ship non-tactical ADP systems. The author has provided a framework which is believed to fit the needs of a small surface ship for non-tactical ADP security. Listed, are those sections deemed applicable, as well as sections which should be added to make the manual more germane to these ships. It is recommended that the task of producing this manual be undertaken by the Surface Force Type Commanders, who have already forseen the need for this type of instruction, and that they should also oversee and implement the program. The new manual should be written so that it is applicable to all small surface ship types, with specific appendices written for specific ship classes. This is a necessary requirement due to the minor differences which exist because of differing security threats. The level of detail required for this manual is determined by the complexity of the necessary requirements. The type of threats to the systems employed are specific and vary by small degrees between ship classes. It is the type of threat which should determine this level of detail.

The type of security organization required for a small surface ship is smaller than that required for a large ADP installation. The author recommends that an ADPSO and ADPSSO be appointed to fill the requirements of this organization. The ADPSO should be on the level of a department head, preferably the Operations Officer. This is due to his already close contact with various aspects of security on the ship, and because the other department heads are already too encumbered with other responsibilities. The

ADPSSO will be the assistant to the ADPSO, and the position should be filled by one of the junior officers. It is imperative that these officers be given adequate training in order to fulfill their responsibilities in a proper manner.

It has been noted that proper training as to the operation of these systems is a key factor in maintaining adequate security. The author recommends that, in addition to the courses being offered at SWOSCOLCOM for Surface Warfare Officers, additional courses be instituted at the Fleet Training Centers and organic training schools to instruct enlisted personnel in the proper use of shipboard non-tactical ADP systems. There is a need to establish PQS for these systems' users to ensure that proper training is obtained.

ADP security is an integral and necessary part of the ADP system. With the advent of new non-tactical ADP systems on small surface ships, it is necessary to ensure that proper steps be taken to guarantee that appropriate measures are instituted for this type of security on the small ships. The recommendations established in this thesis will provide a foundation for what the author believes to be a usable requirements manual and organization hierarchy.

LIST OF REFERENCES

1. Brown, Mark T., "The Computer Gap," US Naval Institute Proceedings, p. 44, December 1984.

2. Department of the Navy, Naval Sea Systems Command, Navy Decision Coordinating Paper for SNAP II, submitted by SAI Comsystems Corporation, McLean, Virginia, p. 1, 5 January 1979.

3. Cox, Gerry M., "Snap II It," Surface Warfare, p.20, March/April 1985.

4. Department of Commerce, National Bureau of Standards, Guideline for Computer Security Certification and Accreditation, FIPS Pub 102, p. 12, September 1983.

5. Ames, Stanley R. and Neumann, Peter G., "Computer Security Technology," Computer, p. 11, July 1983.

6. Department of Commerce, National Bureau of Standards, Guidelines for Automated Data Processing Physical Security and Risk Management, FIPS Pub 31, p.9, June 1974.

7. Department of Commerce, National Bureau of Standards, Guidelines for Security of Computer Applications, FIPS Pub 73, p. 8, June 1980.

8. Faurer, Lincoln D., "Computer Security Goals of the Department of Defense," Computer Security Journal, p. 57, Summer 1984.

9. Courtney, Robert H., "Computer Security Goals of the DOD--Another Opinion," Computer Security Journal, p. 61, Summer 1984.

10. Landwehr, Carl E., "The Best Available Technologies for Computer Security," Computer, p. 86, July 1983.

11. Ames, Stanley R.and Gasser, Morris and Schell, Roger R., "Security Kernel Design and Implementation: An Introduction," Computer, p. 14, July 1983.

12. Fraim, Lester J., "Scomp: A Solution to the Multilevel Security Problem," Computer, p. 26, July 1983.

13. Schell, Roger R., "A Security Kernel for a Multiprocessor Microcomputer," Computer, p. 47, July 1983.

14. Department of the Navy, Naval Sea Systems Command, Purchase Item Description, Data Processing System for SNAP II, submitted by SAI Comsystems Corporation, McLean, Virginia, p. F-24, 20 March 1979.

15. Department of the Navy, Naval Sea Systems Command, Training Support Plan for SNAP II, Draft, submitted by SAI Comsystems Corporation, McLean, Virginia, p. 14, 28 September 1978.

16. Department of the Navy, OPNAVINST 5239.1A, Department of the Navy Automatic Data Processing Security Program, p. 3-6, 3 August 1982.

BIBLIOGRAPHY

Courtney, Robert H. and Orceyre, Michael J., "Considerations in the Selection of Security Measures for Automatic Data Processing Systems," *National Bureau of Standards Special Pub 500-33*, June 1978.

Denning, Dorothy E. and Denning, Peter J., "Data Security," *Computing Surveys*, September 1979.

Department of Commerce, National Bureau of Standards, *Glossary for Computer Systems Security*, FIPS Pub 39, February 1976.

Department of Commerce, National Bureau of Standards, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, FIPS Pub 41, May 1975.

Department of Commerce, National Bureau of Standards, *Guideline for Automatic Data Processing Risk Analysis*, FIPS Pub 65, August 1979.

Department of Defense, DOD Directive 5200.28, *Security Requirements for Automatic Data Processing (ADP) Systems*, 18 December 1972.

Department of Defense Computer Security Center, *DOD Trusted Computer Evaluation Criteria*, CSC-STD-001-83, 15 August 1983.

Department of the Navy, Chief of Naval Material Ser 550-017, *Interim Authority to Operate for all SNAP II Ships and Marine Air Groups*, 20 January 1984.

Department of the Navy, Naval Sea Systems Command, *Preliminary Integrated Logistic Support Plan for SNAP II*, submitted by SAI Comsystems Corporation, McLean, Virginia, 28 September 1979.

Enger, Norman L. and Howerton, Paul W., *Computer Security: A Management Audit Approach*, Amacom, 1980.

Faurer, Lincoln D., "Information Protection in the Federal and Private Sectors," *Computer Security Journal*, Fall-Winter 1983.

Grant, Peter and Riche, Robert, "The Eagle's Own Plume," *US Naval Institute Proceedings*, July 1983.

Harris, Norman L., "Rigid Administrative Procedures Prevent Computer Security Failure," *Data Management*, December 1984.

Head, Robert V., *Federal Information Systems Management*, The Brookings Institution, 1982.

Landwehr, Carl E., "Formal Models for Computer Security," *Computing Surveys*, September 1981.

Martin, James, *Security, Accuracy, and Privacy in Computer Systems*, Prentice-Hall, Inc., 1973

Rushby, John and Randell, Brian, "A Distributed Secure System," *Computer*, July 1983.

Walker, Bruce J. and Blake, Jan F., *Computer Security and Protection Structures*, Dowden, Hutchinson and Ross, Inc., 1977.

Williams, John D., "Leadership in the Computer Age," *US Naval Institute Proceedings*, November 1983

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Superintendent Attn: Library Code 0142 Naval Postgraduate School Monterey, California 93943-5100	2
3.	LCDR Barry Frew, SC,USN Code 54FW Naval Postgraduate School Monterey, California 93943-5100	1
4.	Jack W. LaPatra Code 54LP Naval Postgraduate School Monterey, California 93943-5100	1
5.	Curricular Officer, Code 37 Naval Postgraduate School Monterey, California 93943-5100	1
6.	Lt Joseph E. Zavodny, USN Surface Warfare Officer School Department Head Course Newport, Rhode Island 02841	2

END

FILMED

1-86

DTIC