DEPARTMENT OF THE NAVY
OFFICE OF THE JUDGE ADVOCATE GENERAL
200 STOVALL STREET
ALEXANDRIA, VA 22332-2400

IN REPLY REFER TO

JAGINST 5239.1
63

07 SEP 1990

JAG INSTRUCTION 5239.1

Subj: AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY PROGRAM

Ref: (a) SECNAVINST 5239.2
(b) OPNAVINST 5239.1A

Encl: (1) Information Systems Security Overview
(2) Risk Assessment Documentation Package

1. Purpose. To implement references (a) and (b) within the Office of the Judge Advocate General (OJAG).

2. Discussion. References (a) and (b) establish the Department of the Navy AIS Security Program. The objective of this program is to ensure the availability of mission-essential information by protecting automated computer systems, networks, and computer resources against environmental hazards, misuse or sabotage, and by implementing safeguards to prevent the negligent or unauthorized disclosure, modification, or destruction of data. The program requires the formal accreditation of AISs, networks, and computer resources based on a certification and risk management process.

3. Policy. All AISs, networks, and computer resources within OJAG will be accredited by the Designated Approving Authority (DAA), based on a certification and risk management process. This process requires the identification of threats to data integrity, development of counter-measures for these threats, a means of ensuring continuity of operations should data integrity be violated, and making a decision that a system is operating within an acceptable level of risk.

a. For AISs that are not accredited, the DAA may issue an Interim Authority To Operate (IATO) for a period not to exceed one year.

b. An accreditation or IATO may be issued for an entire system or group of systems in those instances where the DAA has determined that such a "blanket" IATO or accreditation represents the most efficient means of maintaining system operability while ensuring security.

c. Accreditations will be reviewed at least once every three years, or when changes to the functionality, architecture, data processed, user population, or environment may result in increased exposure to harm of the AIS, network, or computer resource. If no changes have taken place, the accreditation may be reissued based upon a thorough review of the previous accreditation documentation.

4. Action.

a. Reference (b) establishes three levels of information processing for security analysis purposes:

Level I - Includes those systems processing classified data;

Level II - Includes those systems not processing classified data, but processing otherwise sensitive information requiring protection from disclosure or modification (i.e. Privacy Act data, financial information, etc.);

Level III - All other systems.

b. The majority of information processing performed in OJAG does not involve classified information. Therefore, the certification requirements need not conform to those necessary for Level I. However, because matters qualifying for Level II classification are routinely handled, a security analysis and certification are required for all systems. Basically, references (a) and (b) require the following steps:

(1) Identify a DAA who must formally certify that appropriate security steps have been taken.

(2) Appoint an Information Systems Security Officer (ISSO). There may be a single ISSO, one per division, or other arrangement as appropriate, provided that ISSO responsibility for all computer and word-processing systems is clearly defined.

(3) Conduct a Risk Assessment -- a formal analysis of the vulnerability of the office's information systems to sabotage, environmental hazards, theft, improper disclosure of information, and other threats to proper operation.

(4) Establish appropriate countermeasures to prevent or minimize the potential damage from the identified threats.

(5) DAA issues a formal accreditation statement in writing that DAA has reviewed the Risk Assessment and has evaluated the established countermeasures and considers them adequate or considers the risks acceptable for the system's use.

c. The Principal Deputy Assistant Judge Advocate General (Operations and Management) is the DAA for OJAG and shall ensure that references (a) and (b) are implemented within OJAG. The DAA is responsible for formally granting authority in writing (accreditation) to operate systems based upon an acceptable level of risk after reviewing the certification and risk management process and the accompanying documentation. Contingency plans shall be tested prior to accreditation or reaccreditation under realistic operational conditions to the maximum extent feasible.

d. The Assistant Head, Information Resources Branch, Management and Plans Division, is the Information Systems Security Officer (ISSO) for OJAG. The ISSO is responsible for developing and implementing an effective risk management program within OJAG that meets the minimum requirements set forth in enclosure (2) of reference (a). The ISSO shall ensure that accreditation support documentation is developed, maintained, and presented to the DAA for review. Enclosures (1) and (2) may be used to assist in this process.

e. Division directors and heads of activities that utilize AISs, networks, or computer resources shall appoint Technical Support Representatives (TSRs) and task them with assisting the ISSO in developing and implementing an effective risk management program within OJAG. This includes risk assessment, security test and evaluation (ST&E), and contingency planning for site-specific AISs. The ISSO shall be kept informed of all TSR appointments and changes as they occur.

J. E. GORDON
Rear Admiral, JAGC, U.S. Navy
Acting Judge Advocate General

Distribution:
JAC (All codes)
NAMARA (All codes)

INFORMATION SYSTEMS SECURITY OVERVIEW

WHAT IS INFORMATION SYSTEMS SECURITY?

Security revolves around three concerns:

1. Classified information and protection of sensitive defense information usually associated with intelligence, command and control, and other equally sensitive functions.

2. Protection of equipment and other resources (supplies, etc.) from loss, theft, physical damage, unauthorized use, and environmental damage such as fire, water, dirt, and dust.

3. Privacy - the protection of personal rights to privacy by safeguarding information.

SECURITY THREATS/THREAT AGENT/VULNERABILITY.

Some of the information security threats that we must deal with in the operation of our information systems are:

1. Unauthorized retrieval or modification of information.

2. Denial of authorized access.

3. Physical damage to or destruction of equipment, storage media (disks) or software.

4. Circumvention of security controls.

5. Theft or compromise of printed system documentation and reports.

6. Browsing - legitimate user attempting to access unauthorized files.

7. Unauthorized duplication of information in files.

8. Unauthorized copying of software prohibited by copyright or license.

VULNERABILITIES

Just as with the threat, the individual sites must take a detai!ed view of their operations to determine their speci.ic vulnerabilities.

When using microcomputers in an office environment, some of the vulnerabilities that you should be concerned with include unauthorized use of personal data, authorized personnel trying to access unauthorized files, theft and unauthorized use of microcomputer equipment, unauthorized modification of information, and other various equipment and software failures.

All personnel using the system should already have a security background evaluation which checks their loyalty, motivation, and morale. System security should depend upon the integrity of as few people as possible.

The next step concerns physical security considerations. This includes the traditional door locks, fire and smoke detectors, access controls, and the guarding against the loss of power and other utilities. The use of surge protectors on your microcomputers and peripherals will be employed to protect your equipment against power surges. We must not only look at the computer terminal, but the building in which it is contained and the immediate environment around the building.

The following is a partial list of these vulnerabilities:

1. PHYSICAL SECURITY.

2. DOCUMENT AND INFORMATION SECURITY - this includes a system of document accountability to include receipt, storage, dispatch and destruction. Information security concerns the protection of classified or privacy data.

3. COUNTER SABOTAGE SECURITY - protecting hardware and software from all forms of sabotage.

4. HARDWARE SECURITY - protecting against theft, destruction, and unauthorized modifications.

5. SOFTWARE SECURITY - protecting against theft, destruction, unauthorized modifications, and unauthorized access.

6. COMMUNICATIONS SECURITY - protecting against interception of communications between terminals.

PROTECTION PROCEDURES

Microcomputers must be protected to the level of the highest classified material processed in order to prevent tampering, visual access to personal material displayed on a screen, and to prevent unauthorized individuals from using the microcomputer in an attempt to gain personal data. Authorized personnel should be made aware of the dangers of having magnets or electromagnetic generating equipment, such as a microwave oven, in the area of computer equipment. The identity of all people who have access to the computers, disks, and printed reports should be known to all authorized personnel. Also, all authorized personnel should be completely familiar with all of the security procedures that are in effect for their particular working environment. When planning access controls, the following factors should be considered: building design, building security, receptionists, door locks, cipher locks, badge and pass systems. personnel indoctrination. access to the console. and the control of visitors or vendors.

DOCUMENTATION AND INFORMATION SECURITY

Document and information security is primarily composed of the broad fields of storage, transmission and dissemination, marking and handling, need-to-know, security control personnel, document accountability systems, and destruction or declassification procedures.

SOFTWARE SECURITY

The areas that should be addressed in regards to software security are:

1. User access.

2. Information access.

3. Denial of access.

4. File classification determination.

5. Input/output limitations.

6. Job security interaction.

COUNTERMEASURES

1. At most large offices, there will be multiple installations of the microcomputer or word processing equipment. Therefore, vulnerabilities involving damage/destruction of equipment may be minimized by arranging contingency use of alternate equipment either in another office or temporary rental from a commercial establishment. Those offices without redundant equipment capabilities are primarily those with small caseloads that may be handled by manual processing as a contingency.

2. Strict observance of data backup procedures will offer protection against most threats to the data storage media. In addition, physical separation and securing of backup and primary media will help protect against deliberate destruction of both sets of data.

3. Because the microcomputer equipment involves pilferable components, steps should be taken to limit access to that equipment or to make the equipment secured using commercially available hardware locking systems. Important diskettes should be stored in lockable fireproof containers if possible, especially where privacy or personal data is involved.

4. The system software must be designed to limit access to data for entry, modification, or retrieval to authorized operators. This involves using multiple-level passwords and changing the password when required and at random points in time.

PROTECTION OF PERSONAL INFORMATION

Several laws and regulations pertaining to the protection of the personal privacy and rights of individuals are applicable to records maintained by Department of the Navy activities. Among these are the Privacy Act, 5 U.S.C. sec. 552a (1982) and SECNAVINST 5211.5C, which prohibit disclosure of information contained in "systems of records" which would constitute a "clearly" unwarranted invasion of personal privacy. The purpose of the Privacy Act is to provide certain safeguards for an individual against an invasion of personal privacy by Federal agencies. These laws and regulations prescribe a variety of requirements with respect to the maintenance of records of personal information, and also provide civil and criminal penalties for violations of those requirements. It is not the purpose of this instruction to address the legal issues attendant to records maintenance and disclosure, but rather to provide a practical guide to their use in the context of office automation systems such as those found in NLSOs. Therefore, the terms "personal data," and "systems of records" are not to be taken in their technical, legal sense, but should be used to generically refer to collection and maintenance of information regarding the sensitive personal affairs of individuals.

SAFEGUARDS

1. Each office shall establish administrative and physical safeguards to protect each system of records from unauthorized or unintentional access, disclosure, modification or destruction. These safeguards shall apply to systems of records in whatever medium in which personal information is processed or stored. Such safeguards shall be tailored to the requirements of each system of records.

2. Access to personal information shall be restricted to those persons whose official duties require access and the individual concerned. The minimum protection to be afforded personal data is that applicable to information classified as "FOR OFFICIAL USE ONLY."

3. Each office shall ensure that all persons whose official duties require access to or processing and maintenance of personal information are trained in the proper safeguarding and use of such information.

4. Personal records and documents shall be stored so as to reasonably preclude unauthorized disclosure.

5. Disposal of records containing personal information which are no longer required will be accomplished in a manner that will prevent the contents from being disclosed (e.g., tearing or shredding the record into pieces, burial or in the case of diskettes, erasure and reformatting).

RULES OF CONDUCT

The following sanctions should be emphasized to all personnel who handle Privacy Act data:

1. There are criminal penalties under the Privacy Act for wrongfully maintaining, disclosing or requesting access under false pretenses to a record subject to the Act. Generally, no disclosure of information from a record about an individual should be made without the written consent or the written request of that

individual, unless disclosure is allowed under certain provisions of the Privacy Act.

2. The agency may be subject to civil suit for failure to comply with the Privacy Act.

HANDLING OF PERSONAL DATA

1. Prepare a procedures handbook which describes the precautions to be used and obligations of computer facility personnel during the physical handling of all personal data. Include a reference regarding the applicability of the procedures to those government contractors who are subject to the Privacy Act.

2. Label all recording media which contain personal dat. Labeling such media will reduce the probability of accidental abuse of such data.

3. Store personal data in a manner that conditions users to respect its confidentiality, e.g., disks kept under lock and key when not being used.

4. If a program generates reports containing personal data, have the program print clear warnings of the presence of such data on the reports.

5. Keep a record of all categories of personal data contained in computer generated reports to facilitate compliance with the requirements that each office identify all such data files and their routine use by the office.

6. Carefully control products of immediate processing steps, e.g.. erase diskettes to ensure that they do not contribute to unauthorized disclosure of personal data.

7. Maintain an up-to-date hard copy authorization list of all individuals (computer personnel as well as systems users) allowed to access personal data for use in access control and authorization validation. Operations and systems personnel should be considered privy to any data they handle since anomalous conditions may cause or require their knowledge of data contents.

8. Maintain an up-to-date hard copy data dictionary listing the complete inventory of personal data files within the computer facility in order to account for all obligations and risks.

9. All court-martial records will contain some personal data that is to be protected under the Privacy Act. Therefore, all court-martial records entered into the microcomputer system will be considered Privacy Act data. The disks that contain the records should be labeled as containing Privacy Act data and afforded the proper security precautions. This labeling procedure will also apply to any back-up diskettes.

DATA PROCESSING PRACTICES

1. Use control numbers to account for personal data upon receipt and during input, storage and processing.

2. Verify the accuracy of personal data acquisition and entry methods employed.

3. Take both regular and unscheduled inventories of all tape and disk storage media to ensure accurate accounting for all personal data.

4. Use carefully devised backup procedures for personal data. A copy of the data should be kept at a second location if its maintenance is required by law.

5. Create a records-retention timetable covering all personal data and stating minimally, the data type, the retention periods, and the authority responsible for making the retention decision.

6. After a computer failure, check all personal data which was being processed at the time of the failure for inaccuracies resulting from the failure.

7. Files created from files known to contain personal data should be examined to ensure that they either do not contain personal data or if they do contain personal data, that they are so labelled and afforded the same security precautions as the original personal data file. A formal process must be established for the determination that such files are releasable as unclassified or released in accordance with established procedures concerning personal data reports.

ASSIGNMENT OF RESPONSIBILITIES

1. Designate the ISSO to be responsible for examining installation practices in storage, use and processing of personal data, including the use of physical security measures, information management practices and computer systems access controls. He/she should consider both internal uses and the authorized external transfer of data, reporting any risks to the relevant management authority.

2. Ensure that all employees engaged in the handling or processing of personal data adhere to established codes of conduct.

SUMMARY OF MANDATORY MINIMUM SECURITY REQUIREMENTS

I. Security Management

A. Appoint a local IS Security Officer
B. Principal Deputy Assistant Judge Advocate General (Operations and Management) is the DAA
C. Instruct authorized personnel in IS security procedures

II. Environmental and Physical Security

A. Temperature and Humidity

1. Equipment operated within manufacturer's suggested range

2. Only authorized personnel handle environmental controls

B. Lighting and Electrical Service

1. Adequate lighting provided
2. Emergency lighting available for safe exit in an emergency
3. Periodic checks of the emergency lighting system
4. All computer equipment plugged into surge protector box(es)
5. Computer equipment not overloading electrical system or plugged into same circuit as coffee pot, heaters, vacuum cleaners, etc.

C. Cleanliness

1. Personnel trained on proper procedures for cleaning

around IS equipment
2. Noncombustible waste baskets
3. Dust and static contributors not a!lowed in equipment area
4. Air-conditioner filters checked re,ularly
5. Floors properly buffed or carefully damp mopped
6. Carpeted area vacuumed regularly and use of anti-static spray if necessary

D. Precautionary Measures Against Water Damage

1. Regular inspection of overhead pipes and false ceiling if applicable
2. Plastic sheets available to cover equipment if necessary

3. Wet equipment will <u>not</u> be turned on until completely dry

E. Fire Safety

1. Periodic training for handling fire emergencies including:
   a. Complete power shutdown
   b. Use of fire extinguishers
   c. Use of fire alarm system
   d. Building evacuation procedures
2. Master control switch to shut off all power to equipment, i.e. surge protected power strip
3. Fire extinguishers -
   a. Clearly displayed
   b. In an easily accessible area
   c. No more than 50 feet from equipment
   d. Only CO2 or Halon fire extinguishers for electrical fires
   e. Properly maintained and checked
4. Smoke detection equipment installed in all required areas
5. Disks stored in fireproof container if economically feasible

F. Physical Protection - refer to OPNAVINST 5510.45B (NOTAL)

1. Physical barriers
2. Surveillance of the controlled area
3. Physical access to data files restricted to individuals with the need-to-know

4. Physical access to the IS equipment area -
   a. Controlled by door locks
   b. Computer equipment secured against theft
   c. List of authorized users
   d. IS equipment isolated from other working areas
5. Effects of natural disasters will be prevented, controlled, and minimized to the extent that is economically feasible
6. Disks kept in their sleeves and locked in some kind of container when not being used

III. Contingency Planning

A. Actions required to minimize impact of damage to or destruction of equipment, storage media and software, i.e. off-site storage of backups and software

B. Development and periodic testing of back-up procedures following disruption in providing essential equipment services C. Development and periodic testing of restoration procedure following physical destruction of equipment and data

IV. Information Security

A. Posted list of authorized equipment users

B. Posted list of personnel who can receive Personal Data Reports

C. Changing a password when a person leaves or if you suspect an unauthorized person may know the password

D. Data disks are kept locked up when not in use

E. Daily disk back-up procedures followed

F. Labeling all disks, reports, and documents that contain Privacy Act data stating that they contain personal data and should be protected

G. Erase and reformat Privacy Act data disks when applicable H. Shredding Privacy Act reports and documents when no longer needed

RISK ASSESSMENT DOCUMENTATION PACKAGE

INFORMATION SYSTEM SECURITY SURVEY

Section I. Basic Data.

1. System Identification: ______________________________

IS Security Officer: ______________________________
Date of Survey: ______________________________

2. System Description: (List all microcomputers, printers, screens, modems, remote devices, network interfaces, and other peripherals)

INFORMATION SYSTEM SECURITY SURVEY

3. Equipment Location: ______________________________

4. System Operations Contact for Security:

Name: ______________________ Code: ______________
Bldg: ____________ Room: ____________ Phone: ______________

5. Types of Data Processed and Security Modes of Operation

TYPE OF DATA	PERCENT OF PROCESSING TIME	SECURITY MODE OF OPERATION
		(i.e., Limited Access)
LEVEL II		
Privacy Act		
For Official Use Only		
Financial		
Sensitive Management		
ːopprietary		
Privileged		
LEVEL II:		

TOTAL 100%

6. Operating System and Standard Applications Software Identifications:

____

____

____

____

INFORMATION SYSTEM SECURITY SURVEY

7. Scope of System: (Check all that apply.)

( ) Single microcomputer and single controlled area.

( ) Shared logic and single controlled area [single CPU with multiple workstations (e.g., 5520)].

( ) Shared logic and more than one controlled area [single CPU with multiple workstations (e.g., 5520)].

( ) Multiple microcomputers and single controlled area.

( ) Multiple microcomputers and more than one controlled area.

( ) Used with a remote computer (i.e., WESTLAW, EMAIL) ____________ percent of time.

( ) Other: ____

8. Total Value of System: $ ________________ (Dollar value impact of loss and cost to replace.)

A. Equipment: $ ____________________

B. Software: $ ____________________

C. Data: $ ____________________

9. Mission Relation:

A. Primary Function(s) of the System or Network:

____

____

____

____

B. Contingency Plan Requirement:

( ) Plan is in existence. Date of plan is ____________________.

( ) Plan is being developed. Estimated completion date is __________________________.

( ) Plan is not required because loss of processing capability for a reasonable period of time would not adversely affect mission. (For example, 2, 4, 8 hours, 2 days, etc. depending on the criticality of the information systems function.) Provide justification.

10. Summary of identified Major Threats or Conditions:

Environmental

Heat/Humidity ___________________________________

Lighting/Electrical ___________________________________

Housekeeping ___________________________________

Water Damage ___________________________________

Fire ___________________________________

Unauthorized Physical Access:

Unauthorized Information Disclosure or Access:

INFORMATION SYSTEM SECURITY SURVEY
APPLICABLE COUNTERMEASURES

SECTION II. Site Security Profile and Minimum Requirements for Environmental and Physical Security. (Applies to all IS Systems and Networks.)

1. Vulnerability: Temperature or Humidity Outside Normal Range.

Operating Countermeasures: (Check all that apply.)

( ) Adequate temperature and humidity controls
( ) Only designated personnel operate controls
( ) Other: ______________________________

2. Vulnerability: Inadequate Lighting or Electrical Service.

Operating Countermeasure: (Check all that apply.)

( ) Adequate primary lighting
( ) Adequate emergency lighting
( ) Periodic checks of emergency lighting
( ) Adequate primary power and outlets
( ) Surge protector power strip for each computer system
( ) Computer equipment is not near a microwave oven

3. Vulnerability: Improper Housekeeping.

Operating Countermeasures: (Check all that apply.)

( ) Routine cleaning schedule is adhered to
( ) Personnel are trained on the proper precautions when cleaning around computer equipment
( ) Air-conditioning filters are cleaned/replaced regularly
( ) Carpet area is vacuumed frequently and anti-static spray is used regularly
( ) Smoking, eating and drinking are not permitted in the immediate vicinity of the computer equipment

4. Threat: Water Damage.

Operating Countermeasures: (Check all that apply.)

( ) Water/Steam pipes are not located above computer equipment
( ) Water/Steam pipes are inspected at regular intervals
( ) Plastic sheets available to cover susceptible equipment

INFORMATION SYSTE' SECURITY SURVEY

5. Threat: Fire.

Operating Countermeasures: (Check all that apply.)

( ) Fire extinguisher in the office
( ) Up-to-date fire drill posted
( ) Periodic fire drills
( ) Training - fire prevention methods
( ) Training - emergency power down procedures
( ) Training - use of fire extinguishers
( ) Training - use of fire alarm system
( ) Training - evacuation plan
( ) Training - individual responsibilities in case of fire
( ) Smoke/heat detectors installed
( ) Emergency exits clearly marked
( ) Fire-proof safe for storing important documents and diskettes or off-site storage available

6. Vulnerability: Unauthorized Physical Access.

Operating Countermeasures: (Check all that apply.)

( ) Building secured outside of normal working hours
( ) Authorized access list
( ) Cipher door lock
( ) Combination door lock
( ) Recognition of authorized personnel
( ) Administrative procedures
( ) Limit the number of personnel who have access to the microcomputer systems data, i.e., need-to-know basis
( ) Privacy Act data diskettes kept in a locked container when not in use
( ) Control of visitors and/or vendors around the computers
( ) Back-up diskettes kept in a different location from the regular working diskettes
( ) Privacy Act reports given out only to those who are authorized to see them
( ) Privacy Act reports shredded when no longer needed
( ) High employee morale
( ) Close supervision of employees
( ) Indoctrination of personnel in security awareness
( ) Other: ____________________
____
____

7. Vulnerability: Improper Compromise of Classified or Sensitive Information.

Operating Countermeasures: (Check all that apply.)

( ) Restrict file access to fewest people with need to know
( ) Erase/reformat disks with sensitive or Privacy Act information when no longer needed
( ) Personnel instructed in proper handing of Privacy Act data
( ) Maintain log of all diskettes, reports etc., containing Privacy Act data
( ) Label or distinctively mark diskettes with Privacy-Act data on them
( ) Passwords for system access changed at random intervals
( ) Lists of authorized users posted at equipment location

8. Other Specific Countermeasures or Contingency Plans: (Describe)

Submitted by: ____________________

Date: ____________________________