MICROCOMPUTER SECURITY SURVEY

AND

MICROCOMPUTER BASELINE SECURITY CONTROLS
RISK ANALYSIS ALTERNATIVE

July 1991

Prepared by:
Naval Computer and Telecommunications Station
Security and Standards Branch

INTENTIONALLY LEFT BLANK

REFERENCES

a. DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs)

b. SECNAVINST 5211.5, Personnel Privacy and Rights of Individuals Regarding Records Pertaining to Themselves

c. SECNAVINST 5239.2, Department of the Navy Automated Information (AIS) Security Program

d. SECNAVINST 5870.5, Permission to Copy Materials Subject To Copyright

e. SECNAVINST 7510.9, Command Management Economy, Efficiency and Review

f. OPNAVINST 5000.52, Command Evaluation Program

g. OPNAVINST 5510.1H, Department of the Navy Information and Personnel Security Program Regulation

h. OPNAVINST C5510.93E, Navy Implementation of National Policy on Control of Compromising Emanations (U)

i. OPNAVINST 5530.14B, Department of the Navy Physical Security and Loss Prevention

j. NRL Report 8897, An Approach to Determining Computer Security Requirements for Navy Systems

k. Public Law 100-235, Computer Security Act of 1987

INTENTIONALLY LEFT BLANK

PREFACE

There is an increasing trend towards developing "baseline" approaches to manage the risks of automated information system environments. This concept proposes upfront implementation of security controls for the most common and already recognized vulnerabilities of an operating environment. The process may eliminate the need to conduct extensive formalized quantitative risk analyses to cost justify protective measures that may be required.

This document, consisting of two parts, was designed and developed as a tool to collect general system information and address the operating risk of a noncomplex microcomputer operating environment. It extracts the pertinent security related information from the instructions and directives in references (a) through (k) to present a composite approach toward analyzing level of risk.

Part I.   Part I is a survey form and uses a fill in the blank approach to gather information about the assets, their processing capabilities, configuration, class of data, mode of operation, system required trust level, and other operating parameters.

Part II. Part II introduces a "baseline" approach to identifying and managing risk. This approach is recommended for use as a risk analysis alternative in low risk environments (e.g., systems processing unclassified, sensitive unclassified, or minimal classified information). The baseline security control concept assumes a basic set of controls, which have been assessed by management, are justifiable for achieving a reasonably secure microcomputer environment. The security control areas identified in Part II are considered fundamental to establishing a baseline of security for a microcomputer operating environment. These controls are designed to counter the threats of human errors, accidents, dishonest and disgruntled employees, and the threats associated with physical and environmental controls.

The "baseline" approach for managing risk, as presented in this document, has been approved for those activities operating microcomputers in a noncomplex environment within the Naval Computer and Telecommunications Command's (NAVCOMTELCOM) Area of Primary Responsibility (APR).

Regardless of the protective measures in place, the key element to security in any microcomputer environment is the user and how well the user follows established computer security policies and guidelines. It can not be overemphasized that users are the ones who help to ensure that the environment is as secure as necessary.

INTENTIONALLY LEFT BLANK

PART I

MICROCOMPUTER SECURITY SURVEY

PART I
PROCEDURES

The procedures identified below are used to complete the microcomputer security survey information in Part I of the document. It is recommended the Automatic Data Processing Systems Security Officer (ADPSSO) assigned to the system gather and record the information.

SECTION I: General AIS Information

This section documents general information about the microcomputer. To complete the form, fill in the blank spaces or check the applicable choice(s) provided as follows:

Item 1. Check the appropriate configuration of the system. If the system is interfaced with another system/network and also used in a stand-alone mode, check both the interfaced configuration and the stand-alone unit areas as provided.

Item 2. Enter the building name/number and room number, if applicable. Indicate if the system is located in government or contractor space.

Item 3. Check the appropriate ownership and type of personnel who operate the system.

Item 4. Enter a check in single user system if the system is assigned to one individual, or check shared system if the system is assigned to and used by more than one individual.

Item 5. Define the classes of information processed on the system and modes of operation. List the percent of processing time for each class of information listed. The total must equate to 100%.

Item 6. List the names of all individuals assigned system responsibilities, their code, and telephone number.

Item 7. List all components, peripherals, communications processors, encryption devices, remote devices and remote interfaces for the system. Include the model number, serial number, and today's replacement cost.

Item 8. List the operating system and version level installed on the system (e.g., MS-DOS, Version 3.30) and today's replacement cost. Check the appropriate software ownership.

Item 9. List the commercial software and version level used on the system (e.g., Word Perfect, Version 5.1; dBase III, Version 1.1; Freelance Plus, Version 3.01; Novell NetWare 386, Version 3.0), appropriate ownership, software serial number, and today's replacement cost.

Item 10. List all customized application software used on the system (i.e., routines and programs developed in-house or by an outside source which contain specific tasks/applications), appropriate ownership, serial number, and today's replacement cost.

Item 11. Enter all letters of certification required for the hardware or software, date, and certification serial number. (Developing agencies must certify safeguards exist for all proposed or existing AISs, operating systems, and application software used for multisite distribution to permit accreditation with minimal effort by the end user commands.) Include in this area TEMPEST letters of certification, if applicable.

Item 12. Enter the total summary value of the equipment, software, and data at today's replacement cost. The value of the data must include disclosure value. The following guidelines are provided for determining the minimum impact of disclosure of sensitive data. These values are based on a per incident of data file disclosure, but do not waive the need for the data owner to determine an accurate estimation of data disclosure.

GUIDELINES FOR IMPACT OF DISCLOSURE OF SENSITIVE DATA

For Official Use Only	$1,000

Privacy Act or Confidential	$10,000
Secret	$100,000
Top Secret	$1,000,000

Item 13. Identify and describe the mission of the microcomputer. Under (a) enter the primary functions or applications processed on the system, and under (b) identify the primary functions or applications processed via an interface with another system or network.

Item 14. Refer to NRL Report 8897 to determine and enter the system's Required Operational Level of Trust (ROTEL). For a given system, five factors must be evaluated to assess the system's overall risk. Based on the risk, the ROTEL can then be determined. The Navy Research Laboratory (NRL) Report 8897 process is used to evaluate each risk factor. The first three factors (local processing capability, communication path, and user capability) focus upon the system's configuration and hardware to determine the System Risk. Risk factors four and five (user clearance and data classification) assess the risk due to the mix of users and information to determine the Data Exposure. System Risk and Data Exposure results yield level of trust, referred to as the ROTEL value.

The NRL Report 8897, titled "An Approach to Determining Computer Security Requirements for Navy Systems," may be ordered from the National Technical Information Service (NTIS) for a charge of $11.00, plus a $3.00 handling charge.

Written requests should reference #ADA155750 and be addressed to:

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

Telephone: (703) 487-4650

Example of determining the ROTEL: System - Zenith 248 Microcomputer

Using the NRL Report 8897 process, the five risk factors are:

Risk Factor 1 - Local Processing Capability Factor is Level 3.
Risk Factor 2 - Communication Path Factor is Level 3.
Risk Factor 3 - User Capability Factor is Level 3.

Each of these factors is applied as follows:

```
Local Processing Capability    =  3      Where the two intersect (on
Communication Path             =  3      NRL Report 8897 Table 1)  =   6

User Capability                =  3
```

Where the 6 and 3 intersect (on NRL Report 8897 Table 2) = 9 for SYSTEM RISK

Risk Factor 4 (Rmin) - User Clearance Factor is Level 1.
Risk Factor 5 (Rmax) - Data Classification Factor is Level 1.

These two factors are applied as follows:

Risk Factor 5 (Rmax) - Risk Factor 4 (Rmin) = Data Exposure*

* If Risk Factor 4 is greater than or equal to Risk Factor 5 data exposure equals 1 (if categories of data are on the system). Otherwise, the data exposure equals 0.

For this example:

```
              (Risk Factor 5)   (Risk Factor 4)
                  Rmax                 Rmin
                    1         -          1     =   0  for  DATA EXPOSURE
```

Refer to NRL Report 8897 Table 3. Use the intersection of the System Risk results (9) and the Data Exposure results (0) to determine the ROTEL value.

For this example:

Security features providing C2 security trust level are required for the Zenith 248.

SECTION II. ACCREDITATION DOCUMENTATION

This section defines the system's current operating status and is to be completed as follows:

Item 1. If the system is operating under an existing accreditation statement, complete paragraph (a). If the system is operating under an interim authority, complete paragraph (b). Provide the following information as applicable:

Paragraph a. Identify the class(es) of data the system processes and mode of operation. Enter the date of accreditation and the name of the individual who granted system accreditation. (Attach a copy of the Statement of Accreditation.)

Paragraph b. Identify the class(es) of data the system is authorized to process and the mode of operation. Enter the date the IATO was issued, expiration date, and the name of the individual who granted the IATO. (Attach a copy of the IATO.)

INTENTIONALLY LEFT BLANK

MICROCOMPUTER SECURITY SURVEY

SECTION I. GENERAL INFORMATION

1. System Identification: (Check all that apply.)

(   ) Microcomputer Used As Stand-alone Unit
(   ) Microcomputer Networked Unit (Internal LAN   External Network   )
(   ) Microcomputer Used To Access System(s) External To The Department
(   ) Other

2. Microcomputer Location: Building: Room:

(   ) Government Space   (   ) Contractor Space

3. System/Hardware is:

(   ) Government Owned/Operated   (   ) Contractor Owned/Operated
(   ) Government Owned/Contractor Operated   (   ) Contractor Owned/Government Operated
(   ) Privately Owned/Operated   (   ) Other

4. The microcomputer is a: (   ) Single User System   (   ) Shared System

5. List the classes of information processed and modes of operation.

Classes of Information	Percent of Processing Time	Modes of Operation *
Classified		
National Cryptologic		
SCI		
SIOP-ESI		
Top Secret		
Secret		
Confidential		
Unclassified (Sensitive)		
Privacy Act		Limited Access
For Official Use Only		Limited Access
Financial		Limited Access
Sensitive Management		Limited Access
Proprietary		Limited Access
Privileged		Limited Access
Unclassified (Not Sensitive)		Limited Access
TOTAL	100%	

* Applicable Modes of Operation For Classified Processing: Partitioned, System High, Dedicated, and Multilevel.

MICROCOMPUTER SECURITY SURVEY

6. System Responsibilities:

	Name	Code	Phone
a. DAA			
b. ADPSO			
c. ADPSSO			
d. NSO			
e. Other			
f. Assigned User(s)			

7. Equipment Description: (List all components, peripherals, communications processors, encryption devices, remote devices, and remote interfaces for

the system.)

Nomenclature/Manufacturer   Model #   Serial #   Cost

8. List operating system, version level, and cost:

(   ) Government Owned (GO)   (   ) Privately Owned (PO)
(   ) Contractor Owned (CO)

9. List commercially used software:

Software/Package Name   (GO/CO/PO)   Serial Number   Cost

MICROCOMPUTER SECURITY SURVEY

10. List Application Software: (Customized for an application.)

Application Name   (GO/CO/PO)   Serial Number   Cost

11. List ALL letters of certification required for hardware and software. (Developing agencies must certify safeguards exist for all proposed or existing AISs, operating systems, and applications software used for multisite distribution to permit accreditation with minimal effort by the end user commands.)

SOFTWARE & HARDWARE TYPE	DATE & SERIAL NUMBER OF LETTER OF CERTIFICATION

12. Total Value of System: (Specify purchase price or equivalent)

Total System Value: $ (Sum of equipment, software, and data)

(Equipment: $ Software: $ Data: $)

13. Mission Relatedness:

A. Identify Primary function(s) of the Microcomputer. (Describe the primary applications processed on the system):

B. Identify Primary function(s) processed via any Network and/or Communication Links, or Distributed Systems.

MICROCOMPUTER SECURITY SURVEY

14. System Security Trust Level Information:

The Required Operational Trust Evaluation Level (ROTEL) for the operating environment of this microcomputer is: (Circle one)

```
Most      A1     B3      B2      B1      C2*      C1      D      Least
Secure  <------------------------------------------------------>  Secure
```

*   SECNAVINST 5239.2, dated 15 Nov 89, requires Class C2 functionality (Controlled Access Protection) computer based security features as defined in DoD 5200.28-STD be implemented by 31 Dec 92.

MICROCOMPUTER SECURITY SURVEY

SECTION II.   ACCREDITATION DOCUMENTATION

1. A current accreditation statement is in existence for this system.

(Check One)

Yes   No

If Yes, complete paragraph (a). If No, complete paragraph (b).

a. Operating under an accreditation statement for processing/handling

data

in

security mode of operation.

Accreditation granted by ,

dated . (Attach a copy of Statement of

Accreditation letter.)

b. This system is operating under interim authority for processing

data in

security mode of operation.

Interim authority granted by

dated . Expires .

(Attach a copy of Interim Authority To Operate)

INTENTIONALLY LEFT BLANK

PART II

MICROCOMPUTER BASELINE SECURITY CONTROL AREAS
RISK ANALYSIS ALTERNATIVE

PART II
PROCEDURES

The procedures identified below are to be used as a risk analysis alternative to analyze the risk level of a microcomputer operating environment. Part II consists of three sections. It is recommended the form be completed by the ADPSSO and reviewed by the Automatic Data Processing Security Officer (ADPSO).

SECTION I. SECURITY CONTROL AREAS

This section contains a basic set of security control areas which are considered fundamental to establishing a secure microcomputer operating environment. Depending on the inherent risk that a given system displays, these baseline controls may not be all inclusive. If in completing this section, it is determined additional security control areas are required to reduce the operational risk, these additional security control areas must be identified and documented. Complete this section as follows:

STEP 1. Request the Designated Approving Authority (DAA) assess the security control areas and approve the use of this baseline approach to quantify the system's level of risk.

STEP 2. Respond to each security control area with a "yes" or "no" answer.

a. If the response is "yes," check the applicable safeguards listed that provide protection to support the security control area requirement. If additional safeguards are implemented, list them in the comments section.

b. If the response is "no," explain, in the comments section, what security deficiencies are evident in the operating environment.

STEP 3. Review the Safeguard Scoring Rationale and assign a score of 1, 2, or 15 for each security control area. A score must be assigned to each security control area. If the security control area does not apply to the operating environment (e.g., TEMPEST Control), assign a score of 1 to indicate a low risk. The score is determined by weighing the implemented safeguards that support the baseline security control area against the requirements of the operating environment.

SECTION II. ANALYSIS OF RISK

This section is used to total the risk rating score for each security control area, assign a risk category, and provide an overall assessment of the operating environment. Complete this section as follows:

STEP 1. Review the responses provided for each security control area and enter the appropriate score in paragraph A., Risk Rating Score, in the score column. Sum the scores of each security control area and enter the total points on the total line provided in paragraph A.

STEP 2. Review the Risk Category Legend and assign the appropriate Risk Category, (Low, Moderate, or High) based on the total scoring points of paragraph A and the applicable scoring range identified in paragraph B.

STEP 3. Based upon your knowledge of the operating environment and any historical data available to you, provide your overall assessment in paragraph C of the AIS operation by responding with a low, moderate, or high risk level. If your overall assessment differs from the risk category assigned in paragraph B, explain the differences in the space provided.

SECTION III. MICROCOMPUTER SURVEY AND SECURITY CONTROL AREA COMPLETION DATA

This section records the name of the individual who completed Parts 1 and 2 and provides recommendations (to be checked as appropriate) based on the risk level identified. Complete this section as follows:

STEP 1. List the name of the individual completing the form, completion date, title/position, location, code, and telephone number. If more than one individual completed the form, list all names.

STEP 2. Based on the data collected and recorded on the document regarding the system's operating environment, any historical data available, and the expertise of the individual(s) completing the form, evaluate the operating environment and check the applicable recommendation.

STEP 3. Sign the form in the space provided. If more than one individual completed the form, their signature(s) is/are also required.

STEP 4. Enter the name, title/position, and telephone number of the individual who reviewed the form. Sign and date the form in the space provided.

INTENTIONALLY LEFT BLANK

MICROCOMPUTER BASELINE SECURITY CONTROLS
RISK ANALYSIS ALTERNATIVE

SECTION I: SECURITY CONTROL AREAS

1. SECURITY CONTROL AREA: System Access Control (Protective measures to ensure
the
identity of each user authorized access to the system is positively established
prior
to granting access.)

Access to the system is controlled to ensure each person having access can be identified and held accountable for their actions.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)

__ An Access Control Policy is in place and enforced.

__ Warning against unauthorized access is displayed.

__ Access control software package is used to provide system access control.

__ Access control hardware/software package is used to provide system access control.

__ Access control token/authentication devices used to provide system access control.

__ Authorized user list posted.

__ Individual user IDs/passwords assigned.

__ Passwords are removed when employee terminates.

__ System is not left on and unattended.

__ Audit Trail is in use and regularly monitored.

__ System is equipped with limited log on attempts

__ Unauthorized system access attempts reported.

__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1
Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level.	2
High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level.	15

2. SECURITY CONTROL AREA: Data Access Control (Data access controls ensures only authorized users having a need to know have access to, knowledge of, or possession of information processed and stored on a system.)

Data files are identified and protected in accordance with appropriate security classification and procedural guidelines.

Yes ______   No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)

__ Least privilege principle followed limiting data access to authorized users.

__ Critical and sensitive data files are identified and protected.

__ Storage of sensitive data on the hard disk is prohibited.

__ Procedures to ensure data integrity have been established to prevent accidental or malicious modification, unauthorized disclosure or destruction of data.

__ Color coded labels are used to comply with Information Security Oversight Office standard color code label requirements.

__ Application programs written with feature that permits only authorized users access to data.

__ Removable media only used and properly secured.

__ Output products properly marked.

__ Backup copies of critical data files created regularly.

__ An off-site area is used for backup storage of critical data.

__ Password control procedures are implemented.

__ Passwords are protected and changed frequently (at least monthly).

__ Employees log off before leaving system unattended.

__ Personnel periodically informed of their information security responsibilities.

__ Physical access controls to the microcomputer area are enforced.

__ Sensitive data files are encrypted when not actually used.

__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1
Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level.	2
High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level.	15

3. SECURITY CONTROL AREA: Software Control   (Software control ensures software integrity is maintained and only authorized software is used on the system.)

Controls are in place to ensure integrity and protection of all software used on the system.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Proprietary software procedures implemented and enforced to ensure compliance with copyright/license laws.
__ All personnel are made aware of the command's policy on reproducing copyright software.
__ Use of unapproved software from any source is prohibited.
__ All new software is checked for possible infection before installation.
__ Original software is stored in a secure location outside the micro area.
__ Backup copies are appropriately maintained.
__ An inventory is maintained of all software assigned to the system.
__ Documentation available for application software developed in-house.

__ Configuration control procedures have been established to control software modifications.
__ Virus detection software is available to detect malicious code.
__ Virus detection software is used on a regular basis to detect malicious code.
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale: Score

Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level. 1

Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level. 2

High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level. 15

4. SECURITY CONTROL AREA: Physical Security Control (Physical security controls safeguard personnel, prevent unauthorized access to sensitive or critical areas, and provide protection against espionage, sabotage, damage and theft.)

The microcomputer is located in an area with good physical access controls.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Locks on door(s) to microcomputer area.
__ Building secured after normal working hours.
__ Equipment cover lock or equipment lockdown devices utilized.
__ Power switch lock installed on system.
__ Individual badge system in use.
__ Escort and visitor control procedures implemented.
__ Security guards on duty.
__ Electronic alarms and monitoring devices used.
__ Personal belongings searched on entering and leaving the building.
__ Strangers entering the micro area are challenged.
__ Warning signs posted indicating boundaries of restricted areas.
__ Closed circuit television system (CCTV) installed.
__ Additional safeguards implemented (list in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1
Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level.	2
High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level.	15

5. SECURITY CONTROL AREA: Environmental Controls (Protection measures to prevent, detect and minimize the effects of hazards such as fire, water damage, air contaminants, excess heat and electricity brownouts.)

Environmental hazards to which the microcomputer is exposed are minimized.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Functioning fire detection system or smoke alarm installed in microcomputer area.
__ Hand held Halon fire extinguishers are readily available.
__ Fire extinguishers are regularly inspected.
__ Sprinkler system installed.
__ Emergency exits are clearly marked.
__ Periodic fire drills conducted.
__ Personnel trained in local fire fighting policy.
__ Micro connected to isolated power source.
__ Micro and peripherals plugged into surge protector with three prong outlets, connected to a power director device, or (if micro is subject to frequent power outages) a battery backup/UPS is installed.
__ Adequate primary lighting provided.
__ Emergency lighting provided.
__ Drastic changes in humidity/temperature avoided.
__ Micro located in an area with good air circulation (vents not blocked/air flow unrestricted).
__ Routine cleaning schedule adhered to.
__ Micro kept clear of paper stacks and other flammable materials.
__ Smoking, eating and drinking is prohibited in and around the micro area.
__ Plastic sheeting available to protect micro from dust and water damage.
__ Static electricity is controlled.
__ Users held responsible for maintaining a clean working environment.
__ Additional safeguards implemented (list in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1

Moderate Risk. System can be operated under its present condition.   2
All safeguard requirements are implemented and usually enforced to
operate the system at an acceptable level.

High Risk. System is rejected. Existing safeguards are inadequate   15
for reducing the probability of loss, or the impact of loss, to an
acceptable level.

6. SECURITY CONTROL AREA: Media Handling Controls   (Measures to protect and secure storage media, i.e., source documents, diskettes, hard disks, printouts, tapes, cartridges.)

Media handling procedures have been established and are enforced ensuring all media is handled, stored and backed up properly.

Yes ______   No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Diskettes are protected from dust and dirt, cigarette smoke and ashes, liquid spills, and food crumbs.
__ Care is taken to never touch the recording surface of the diskette.
__ Diskettes are protected from all sources of magnetism.
__ When not in use, diskettes are kept in their protective jackets.
__ A felt tip pen is used to complete label prior to affixing to diskette.
__ Floppy diskettes are protected from bending and similar damage.
__ Diskettes are not subjected to intense heat or intense cold.
__ Employees are instructed to never insert/remove a diskette when the drive light is on to avoid read/write head damage.
__ Diskettes are placed in their protective jackets and stored vertically inside an appropriate container.
__ All magnetic media is externally marked with appropriate markings.
__ When several files are stored on one diskette, a printout of the diskette's directory is taped to the jacket for easy referencing.
__ Storage boxes are kept away from all sources of electromagnetic interference.
__ Procedures for backing up floppy diskettes and hard disks have been developed and routinely followed.
__ Master diskettes are protected by write/protect tabs.
__ The SHIP or PARK command is executed when storing/transporting hard disks.
__ Appropriate procedures are followed for disposing of storage media.
__ NSA approved degaussing equipment utilized.
__ Additional safeguards implemented (list in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1
Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level.	2
High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level.	15

7. SECURITY CONTROL AREA: Personnel Security Control   (Personnel security controls ensure an employee's level of trustworthiness is commensurate with their duties, all personnel are informed of information security requirements including their individual responsibilities, and are made aware of ethical computer behavior practices.)

Appropriate security clearance procedures are followed and all personnel have a current working knowledge of good computer security practices, information security procedures and understand their individual computer security responsibilities.

Yes ______   No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Personnel security policies require screening of all individuals (including contractors) participating in the design, operation, and maintenance of the system or having access to the data in the system, commensurate with the sensitivity of information being handled.
__ New employees are indoctrinated to their ethical responsibilities.
__ Personnel dealing with sensitive information are provided periodic security briefings.
__ Personnel sign a statement that they understand their information security responsibilities.
__ Employees are aware of the command's policy on use of personal resources to perform government work.
__ Personnel security policies include checkout procedures that deny access to the computer system to departing employees.
__ Standard debriefing procedures are followed.
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1
Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level.	2
High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level.	15

8. SECURITY CONTROL AREA: Contingency Planning   (Contingency planning consists of those activities undertaken in the anticipation of potential events which could cause serious adverse effects interrupting normal operations.)

A contingency plan has been developed with documented planned action steps to be taken before, during and after an emergency condition.

Yes ______   No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)

__ Contingency plan prioritizes work based on criticality of functional applications.
__ Backup copies of critical files created regularly.
__ Backup copies of critical files, software packages and original application programs are stored off-site and can be retrieved within a reasonable time frame.
__ When the system is not available, loaner equipment is used.
__ Spare equipment is available for backup operations.
__ Backup operations include an agreement with another facility.
__ During contingency situations, critical processing is performed manually.
__ All personnel involved have been informed of their contingency planning responsibilities.
__ A copy of the contingency plan is stored off-site.
__ The contingency plan is tested and evaluated on an annual basis.
__ The contingency plan is tested under realistic operational conditions.
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1
Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level.	2
High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level.	15

9. SECURITY CONTROL AREA: Computer Security Training   (Training for all employees designed to heighten and maintain a level of security awareness throughout the command to ensure employees understand the criticality of protecting systems and data.)

Mandatory periodic training in computer security awareness and accepted computer security practices, as required by the Computer Security Act of 1987, is provided all employees involved with the management, use, or operation of the system.

Yes ______   No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ An activity Security Training Program has been implemented which provides formal and informal training for all employees.
__ New personnel are briefed on computer security awareness.
__ Computer security films are available and shown to all employees on a scheduled basis.
__ Posters to enhance computer security awareness are posted in heavily trafficked areas.
__ Employees are debriefed on AIS security policies upon departing.
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale:	Score
Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level.	1
Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level.	2
High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level.	15

10. SECURITY CONTROL AREA: Administrative Controls (Administrative controls consist of local policies and guidelines for protecting systems and ensuring compliance with AIS Security Program requirements.)

Detailed Standard Operating Procedures (SOPs) and documentation are provided to establish local policy/guidance and to ensure compliance with program objectives.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Standard Operating Procedures establishing local computer security policies are readily available and maintained in a current status.
__ Acquisition and procurement documentation is reviewed by the ADPSO for compliance with Life Cycle Management program requirements.
__ Security violation procedures have been established and distributed to all personnel.
__ Procedures are established and enforced to safeguard software and files used to provide internal security controls, passwords or audit trails.
__ The activity has established a policy for use of privately owned resources to perform government work.
__ Procedural guidance for reducing the risk of malicious code has been established and made available to applicable personnel.
__ Periodic reviews are performed on the system.
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale: Score

Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level. 1

Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level. 2

High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level. 15

11. SECURITY CONTROL AREA: Class C2 Security (Class C2 security provides for controlled access protection for systems processing classified and sensitive unclassified information. Class C2 security and accountability features are discretionary access control, object reuse, identification and authentication, and audit trail capability.)

The microcomputer is protected by hardware, software, and security operating procedures to provide reasonable security until such time as effective C2 Class protection become available for microcomputers.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Access to information controlled on an individual basis to ensure only having a need-to-know are granted access.
__ Individuals identified and authenticated through User ID and password.
__ A security software package is used to provide C2 functionality (i.e., discretionary access control, object reuse, identification and authentication, and audit trail capability).
__ Overwrite routines are used to clear internal memory and registers.
__ The micro is turned off to clear memory before reuse by another user.
__ Application programs perform a "zero out" function prior to program termination.
__ A manual audit trail is maintained to record each event (date and time of the event, user, type of event).
__ The operating system controls access to all system resources.
__ C2 assurance and documentation requirements (i.e., system architecture, system integrity, security testing, security features user guide, trusted facility manual, test and design documentation) are met through in-house Standard Operating Procedures (SOPs).
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale: Score

Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level. 1

Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level. 2

High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level. 15

Note: This page must be completed if the system is operating in other than a stand-alone mode.

12. SECURITY CONTROL AREA: Communications Security Control (Measures to protect information transmitted over communication lines to ensure the data is not disclosed or compromised.)

Communications lines and links for systems operating in other than a stand-alone mode are secure commensurate with the class of data transmitted.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ Communication wiring contained within approved conduits.
__ Telephone junction boxes/connection points are within controlled spaces.
__ Dedicated transmission lines are utilized.
__ Security modems are installed.
__ Encryption devices are used to protect confidentiality of information.
__ Host-User Agreements in place prior to connectivity.
__ All access attempts are logged.
__ Invalid access attempts are reported.
__ Password management program established to assign, delete, and ensure users change passwords according to policy.
__ Dial-up access connections are protected (i.e., dial-up access restricted to authorized users, dial-up telephone numbers restricted, dial-up lines are monitored, dial back employed once connection has been made).
__ Remote Security Operating Procedures in place and enforced.

__ Hardware/software configuration changes are controlled.
__ Communications Control Manager monitors users' security practices.
__ Audit trail of system activity is regularly reviewed.
__ Procedures implemented for disconnecting from outside connectivity when operating in a stand-alone mode.
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale: Score

Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level. 1

Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level. 2

High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level. 15

Note: This page must be completed if the system is processing classified information.

13. SECURITY CONTROL AREA: TEMPEST Control (Measures to protect against spurious signals, referred to as electromagnetic emanations, emitted by computers that can be intercepted and automated information read.)

The system is in compliance with the TEMPEST requirements of OPNAVINST C5510.93.

Yes ______ No ______ (No answers must be explained.)

Safeguards implemented include: (Check applicable safeguards.)
__ TEMPEST Vulnerability Assessment Request (TVAR) submitted to Commander, Naval Investigative Services Command.
__ Microcomputer TEMPEST approved.
__ TEMPEST waiver received.
__ Filters installed on computer power and phone lines.
__ Protected Distribution System (PDS) installed for processing classified data.
__ PDS approval request submitted.

__ PDS approval received.
__ No radar/microwave or power transformers in general area of computer.
__ Additional safeguards implemented (list below in comments section).

Comments:

Safeguard Scoring Rationale: Score

Low Risk. System accepted as is. All safeguard requirements are implemented and are consistently enforced to operate the system at an acceptable level. 1

Moderate Risk. System can be operated under its present condition. All safeguard requirements are implemented and usually enforced to operate the system at an acceptable level. 2

High Risk. System is rejected. Existing safeguards are inadequate for reducing the probability of loss, or the impact of loss, to an acceptable level. 15

SECTION II: ANALYSIS OF RISK

A. RISK RATING SCORE (A score must be assigned to each security control area.)

Security Control Area	Score	Security Control Area	Score
System Access Control	_____	Contingency Planning	_____
Data Access Control	_____	Computer Security Training	_____
Software Control	_____	Administrative Controls	_____
Physical Access Control	_____	Class C2 Security	_____
Environmental Control	_____	Communications Security	_____
Media Handling Control	_____	TEMPEST Control	_____
Personnel Security Control	_____		
		Total	________

B. RISK CATEGORY

Scoring Range	Risk Category* (Circle One)
---13---	LOW

14 - 26	MODERATE
27 & Above	HIGH

* Risk Category Legend:

Low risk. The system is operating at an acceptable level of risk (adequate safeguards are implemented and enforced for all baseline security control areas).
Moderate risk. The system can be operated under its present condition (adequate safeguards are implemented and usually enforced for all baseline security areas).
High risk. Deficiencies were found in baseline security control areas. Interim Authority to Operate (IATO) issued pending implementation of required safeguards).

C. OVERALL ASSESSMENT

1. Based on your knowledge of the operating environment, and any historical data available, provide your assessment of the AIS operation. (Circle One)

   Low Risk   Moderate Risk   High Risk

2. If your assessment differs from the risk category assigned above, explain in the space provided below.

SECTION III. MICROCOMPUTER SURVEY AND SECURITY CONTROL AREA COMPLETION DATA

1. Completed by:

   Name: Date:

   Title/Position:

   Building: Room:

   Code: Phone:

2. Recommendations: (Check applicable recommendation.)

Recommend Accreditation.

Non-Accreditation recommended until such time as the following safeguards are implemented:

Recommend an in-depth quantitative risk analysis be performed on the system due to high risk areas in the operating environment.

Other (explain):

Signature:

3. Reviewed by:

Name: Date:

Title/Position: Phone:

Signature:

INTENTIONALLY LEFT BLANK