OPNAVINST 5239. IA

RISK ASSESSMENT MATRIX

THREAT	ASSETS AND THEIR IMPACT VALUE														TOTAL ALE BY INDIVIDUAL THREAT
	(a)		(b)		(c)		(d)		(e)		(f)		(g)		
	Hardware		Soft Ware		DATA		Physical Facility		Personnel						
	$ 6,753.00		$ 3,080.00		$ 3,000.00		$ 15,000.00		$ 11,192.00		$		$		
	TV*		TV		TV		TV		TV		TV		TV		
1. Software Alteration	L	20.26	L	9.24	L	9.00	L	45.00							83.50
2. Hardware failure	L	20.24	L	9.24	L	9.00	L	45.00							83.50
3. Backup Data	L	20.26	L	9.24	L	9.00	L	45.00							83.50
4. Operator Error	L	20.26	L	9.24	L	9.00	L	45.00							83.50
5. Data Entry Error	L	20.26	L	9.24	L	9.00	L	45.00							83.50
6. Power Instability	L	20.26	M	101.64	L	9.00	L	45.00							125.90
7. Backup DATA	L	20.26	L	9.24	L	9.00	L	45.00							83.50
8. Unauthorized Disclosure			L	9.24	M	99.00									108.24
9. Training/Procedures			L	9.24	L	9.00									18.24
10. Fire	L	20.26	L	9.24	L	9.00	L	45.00	L	33.57					117.07
11. Theft	L	20.26	M	101.64	M	99.00									220.90
12. Backup/Procedures	L	20.26	L	9.24	L	9.00	L	45.00							83.50
13. Water Damage	L	20.26	L	9.24	L	9.00	L	45.00							83.50
14. Natural Disaster	L	20.26	L	9.24	L	9.00	L	45.00	L	33.57					117.07
15. Failure Environmental	L	20.26	L	9.24	L	9.00	L	45.00	L	33.57					117.07
16. Misuse of Resources	M	222.85	M	101.64	M	99.00									423.49
17. Training/Prcedures	L	20.26	L	9.24	L	9.00									38.50
18.															
19.															
20.															
21.															
22															
23.															
24.															
TOTAL ALE BY INDIVIDUAL ASSET	506.49		341.88		423.00		540.00		100.71						TOTAL ALE 1,912.08

OPNAV 5239/12 (2-82)

* TV (THREAT VALUE) L (LOW) M (MEDIUM) H (HIGH)

OPNAVINST 5239.1A

ADDITIONAL COUNTERMEASURES SELECTION WORKSHEET

A. ADDITIONAL COUNTERMEASURES	B. THREATS PAIRED	C. ORIGINAL ALE	D. REVISED ALE	E. ANNUAL SAVINGS	F. ANNUAL COST OF ADDITIONAL COUNTERMEASURES	G. RETURN ON INVESTMENT	H. ADDITIONAL COUNTERMEASURES PRIORITIES
1. Operating Procedures	(a) misuse	(a) 423.49	(a) 83.50	(a) 339.99			
	(b) Theft	(b) 220.90	(b) 83.50	(b) 137.40			
	(c) u/Discl	(c) 108.24	(c) 18.24	(c) 90.00			
	(d)	(d)	(d)	(d)			
	ANNUAL SAVINGS SUBTOTAL			(e) 567.39	(e) 141.79	(e) 4:1	(e) 3
2. Backup DATA	(a) theft	(a) 220.90	(a) 83.50	(a) 137.40			
	(b) PW/INST	(b) 175.90	(b) 83.50	(b) 92.40			
	(c) Hard/fail	(c) 83.50	(c) 83.50	(c) —0—			
	(d)	(d)	(d)	(d)			
	ANNUAL SAVINGS SUBTOTAL			(e) 229.80	(e) 146.40	(e) 2:1	(e) 1
3. Operator Training	(a) misuse	(a) 423.49	(a) 18.24	(a) 405.25			
	(b) u/Discl	(b) 108.24	(b) 38.50	(b) 69.74			
	(c)	(c)	(c)	(c)			
	(d)	(d)	(d)	(d)			
	ANNUAL SAVINGS SUBTOTAL			(e) 474.99	(e) 18.93	(e) 25:1	(e) 2
4.	(a)	(a)	(a)	(a)			
	(b)	(b)	(b)	(b)			
	(c)	(c)	(c)	(c)			
	(d)	(d)	(d)	(d)			
	ANNUAL SAVINGS SUBTOTAL			(e)	(e)	(e)	(e)
5.	(a)	(a)	(a)	(a)			
	(b)	(b)	(b)	(b)			
	(c)	(c)	(c)	(c)			
	(d)	(d)	(d)	(d)			
	ANNUAL SAVINGS SUBTOTAL			(e)	(e)	(e)	(e)

Sgl

ADP SECURITY SURVEY

SECTION I. Basic Data. (Applies to all ADP systems, networks, and OISs)

1. System Identification: ZCAPS

   ( ) Office Information System

   (X) ADP System

   ( ) Network

2. System Description: (List all components, main frames, peripherals, communications processors, encryption devices, remote devices, network and remote interfaces, etc.)

   Equipment location: Bldg 80. Camp Lejeune,
   North Carolina
   Contact for Security - Sylvia J. Ross
   Bldg 80, Camp Lejeune, N.C. AD-484-5919
   One Z-248 microcomputer w/20 MB
   Hard Drive & One floppy Disk Drive,
   One Epson FX 286 Printer.

FIGURE E-1 (Page 1 of 10)

ADP SECURITY SURVEY

3. Equipment Location: Bldg 80, Camp Lejeune, N.C.

4. System Operations Contact for Security:

Name: Sylvia A. Koss Code: ______

Bldg: 80 Room: ______ Phone: AV-484-5919/5131

5. Types of Data Processed and Security Modes of Operation

TYPE OF DATA	PERCENT OF PROCESSING TIME	SECURITY MODE OF OPERATION*
Level I		
SCI		
SIOP-ESI		
TOP SECRET		
SECRET		
CONFIDENTIAL		
Level II		
Privacy Act		
For Official Use Only		
Financial	100%	Limited Access
Sensitive Management		
Proprietary		
Privileged		
Level III		
TOTAL	100%	

(Note: Applicable security modes are: Compartmented, Controlled, Dedicated, System High, Multilevel, Limited Access, as defined in Appendix A of this manual.)

FIGURE E-1 (Page 2 of 10)

ADP SECURITY SURVEY

6. Operating System and Standard Applications Software Identifications:

____

____

____

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

(✓) Stand-alone and single controlled area (single CPU with single workstation).

( ) Shared logic and single controlled area (single CPU with multiple workstations).

( ) Shared logic and more than one controlled area (single CPU with multiple workstations).

( ) Multiple processors and single controlled area (multiple CPUs).

( ) Multiple processors and more than one controlled area (multiple CPUs).

( ) Used with a remote computer __________ percent of time.

( ) Other: ______________________________

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

A. Equipment: $ ______________

B. Software: $ ______________

C. Data: $ ______________
(Note: Dollar values in Table E-2 can be used as a guideline for computing value of data files.)

ADP SECURITY SURVEY

9. Mission Relatedness

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 ADP function.) Provide justification.

Section II. Site Security Profile and Minimum Requirements for Environmental and Physical Security. (Applies to all ADP systems, networks, and OISs.)

1. Vulnerability: Temperature or Humidity Outside Normal Range.

Operating Countermeasures: (Check all that apply.)

(✓) Adequate heating and controls
(✓) Adequate cooling and controls
(✓) Only designated personnel operate controls
( ) Functioning temperature and humidity recorder
( ) Functioning temperature/humidity warning system
( ) Other: __________________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

FIGURE E-1 (Page 4 of 10)

ADP SECURITY SURVEY

2. Vulnerability: Inadequate Lighting or Electrical Service.

Operating Countermeasures: (Check all that apply.)

(✓) Adequate primary lighting
(✓) Adequate emergency lighting
(✓) Adequate periodic checks of emergency lighting
(✓) Adequate primary power and outlets
( ) Functioning power filters or voltage regulators
( ) Available backup power
( ) Other: ______________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

3. Vulnerability: Improper Housekeeping.

Operating Countermeasures: (Check all that apply.)

(✓) Routine cleaning schedule is adhered to
( ) Cleaning personnel are trained in computer room procedures
(✓) An ADP facility representative is present during cleaning
(✓) Dust contributors are not permitted in equipment areas (outer coats, throw rugs, drapes, venetian blinds, etc.)
(✓) Air-conditioning filters are cleaned/replaced regularly
(✓) Floors are polished with non-flake wax using proper buffer materials or properly damp-mopped
(✓) Carpet areas are vacuumed frequently and anti-static spray is used regularly
(✓) Smoking, eating, and drinking are not permitted in equipment areas
( ) Other: ______________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

ADP SECURITY SURVEY

4. Threat: Water Damage.

Operating Countermeasures: (Check all that apply.)

(✓) Water/steam pipes are not located above equipment
( ) Water/steam pipes are inspected at regular intervals
( ) Functioning humidity warning system
( ) Dry-pipe sprinkler system
( ) Raised floor
(✓) Plastic sheets available to cover susceptible equipment
( ) Water detection devices
( ) Other: ____________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

5. Threat: Fire.

Operating Countermeasures: (Check all that apply.)

(✓) Up-to-date fire bill posted
(✓) Periodic fire drills
(✓) Training--fire prevention methods
(✓) Training--emergency power down procedures
( ) Trainng--knowledge of fire detection system
(✓) Training--use of fire extinguishers
(✓) Training--use of fire alarm system
(✓) Training--evacuation plan
(✓) Training--individual responsibilities in case of fire
(✓) Functioning emergency power-off switches
( ) Sprinkler system installed
( ) Halon system installed
( ) Carbon dioxide fire extinguishers installed
(✓) Smoke/heat detectors installed
(✓) Functioning fire alarm system
(✓) Emergency exits clearly marked
( ) Other: ____________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

FIGURE E-1 (Page 6 of 10)

ADP SECURITY SURVEY

6. Vulnerability: Unauthorized Physical Access.

Operating Countermeasures: (Check all that apply.)

(✓) Perimeter fence
(✓) Security guards
(✓) Building secured outside of normal working hours
( ) Area alarms (motion detectors, open door detectors, perimeter penetration detectors)
(✓) Authorized access list
( ) Cypher door lock
( ) Combination door lock
(✓) Recognition of authorized personnel
( ) Closed circuit television
(✓) Administrative procedures
( ) Physical isolation/protection
( ) High employee morale
(✓) Close supervision of employees
(✓) Indoctrination of personnel in security awareness
( ) Other: ________________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

SECTION III. Current status of accreditation support documentation. (Applies to all ADP activities and networks which will be authorized to handle Level I or Level II data.)

1. All ADP activities and networks which will be authorized to handle Level I or II data must either be accredited or be granted interim authority to operate pending accreditation. Accreditation is based on supporting documentation including a risk assessment. This section provides a statement of the current status of the accreditation support documentation. (Check all that apply.)

ADP SECURITY SURVEY

________________ In existence
______________ Being developed
__________ Required but no action taken
_______ Not required

(✓) ( ) ( ) ( ) Security Operating Procedures Handbook
( ) ( ) ( ) (✓) Line diagrams showing interconnection of components and physical layout
(✓) ( ) ( ) ( ) Description of countermeasures in place
( ) ( ) ( ) (✓) Copies of previous accreditation or interim authority to operate
( ) ( ) ( ) (✓) TEMPEST accreditation request
( ) ( ) ( ) (✓) TEMPEST accreditation test results
( ) ( ) ( ) (✓) Physical accreditation
(✓) ( ) ( ) ( ) ST&E Test Plan
(✓) ( ) ( ) ( ) Contingency Plan
(✓) ( ) ( ) ( ) Contingency Plan test results
(✓) ( ) ( ) ( ) Formal Risk Assessment
( ) ( ) ( ) ( ) Other (specify): ______________________

SECTION IV. Countermeasure Documentation for Office Information Systems. (Applies to all OISs which will be authorized to handle Level I or Level II.)

1. OISs Handling Level II Data. (Check all that apply.)

( ) The OIS will be authorized to handle Level II data. A list of the operating countermeasures is attached. These countermeasures provide proper data protection and audit trails.

( ) The OIS is a shared logic system with more than one simultaneous user not having need-to-know for all data within the system. Password protection or other equivalent countermeasures are employed for system access and for individual file access.

( ) The OIS Security Operating Procedures have been documented and approved.

FIGURE E-1 (Page 8 of 10)

ADP SECURITY SURVEY

2. OISs handling Level I Data. (Check all that apply.)

( ) The OIS will be authorized to handle Level I data under a system high or dedicated mode of operation. A list of the operating countermeasures is attached. These countermeasures satisfy security requirements.

( ) TEMPEST accreditation has been requested. Request date __________.

( ) TEMPEST accreditation has been received. Accreditation date __________.

( ) The OIS Security Operating Procedures have been documented and approved.

SECTION V. Survey Data. (Applies to all ADP systems, networks, or OISs.)

1. Current Status: (Check all that apply.)

( ) Operating under accreditation for processing Level __________ data in __________ security mode of operation. Accreditation granted by ______________. Dated __________. (Attach a copy of statement of accreditation.)

( ) Operating under interim authority for processing Level __________ data in __________ security mode of operation. Interim authority granted by ______________. Dated __________. Expires __________. (Attach a copy of interim authority to operate.)

2. Survey Prepared By:

Name:____________________________ Code:_________________

Bldg:__________ Room: __________ Phone:_________________

FIGURE E-1 (Page 9 of 10)

ADP SECURITY SURVEY

To the best of my knowledge, the information provided in this survey and the attached documentation is complete and accurate.

Signature ______________________________ Date _____________

(Provide a list of all survey team members.)

FIGURE E-1 (Page 10 of 10)

ST&E CHECKLIST 5 JUN 1987

2 Cops

SECTION I

ACTIVITY

	YES	NO	N/A
1. Has an ADP Security Program been established?	✓		
Comments:			
2. Has an Activity ADP Security Plan (AADPSP) been developed?	✓		
Comments:			
3. Has the AADPSP been approved by the Naval Data Automation Command (NAVDAC) Code 51?	✓		
Comments:			
4. Has the Designated Approving Authority granted activity accreditation?		✓	
Comments:			
5. Is the AADPSP updated as changes occur?	✓		
Comments:			
6. Is there evidence that top-level management supports the ADP Security program through such requirements as security awareness training, documented security procedures, etc.?	✓		
Comments:			
7. Is the ADP security staff sufficient to support the ADP Security Program?	✓		
Comments:			

YES NO N/A

8. Has an ADP Security Officer (ADPSO) been appointed in writing by the Commanding Officer? ✓ ___ ___

Comments: ____________________

9. Does the ADPSO have a strong technical background and experience in the administration of ADP systems? ___ ✓ ___

Comments: ____________________

10. Has the ADPSO received training on OPNAVINST 5239.1A? ___ ✓ ___

Comments: ____________________

11. Have the duties and responsibilities of the ADPSO been defined in writing? ___ ✓ ___

Comments: ____________________

12. Do the duties and responsibilities of the ADPSO include:

a. Coordinating with the command security manager on matters concerning ADP security, in accordance with the security organizational structure established by the Commanding Officer? ✓ ___ ___

Comments: ____________________

b. Developing and maintaining an ADP Security Plan (ADPSP)? ✓ ___ ___

Comments: ____________________

c. Ensuring that a Network Security Officer (NSO) is appointed for networks which are sponsored by the activity? ✓ ___ ___

Comments: ____________________

	YES	NO	N/A
d. Ensuring that ADP System Security Officers (ADPSSOs) are appointed in writing where applicable?	___	___	✓
Comments: ______________________			
e. Ensuring that Terminal Area Security Officers (TASOs) are appointed where applicable for each remote facility?	✓	___	___
Comments: ______________________			
f. Ensuring that an effective activity Risk Management Program is implemented?	✓	___	___
Comments: ______________________			
g. Ensuring that all ADP security incidents or violations are investigated, documented and reported to appropriate authorities?	✓	___	___
Comments: ______________________			
h. Ensuring that security requirements are included in life cycle management documentation as prescribed in SECNAV Instructions 5000.1A or 5231.1A as appropriate?	✓	___	___
Comments: ______________________			
i. Ensuring that all procurement documents or specifications approved within the activity comply with ADP security requirements?	✓	___	___
Comments: ______________________			
j. Ensuring the contracts (DD Form 254) include statement(s) ensuring contractor compliance with Navy ADP Security requirements?	✓	___	___
Comments: ______________________			

5 JUN 1987

	YES	NO	N/A
k. Ensuring the development and testing of all contingency plans?	✓		
Comments: ______________________________			
l. Ensuring the NAVAUDSVC is advised of the development of an ADP system, as applicable?	✓		
Comments: ______________________________			
m. Ensuring that accreditation documentation is developed and maintained?	✓		
Comments: ______________________________			
n. Assisting the ADP security staff in implementing their respective ADP security requirements?	✓		
Comments: ______________________________			
o. Ensuring that applicable personnel security procedures are established?	✓		
Comments: ______________________________			
p. Ensuring that Security Test and Evaluations (ST&Es) are conducted where applicable?	✓		
13. If this activity sponsors a network:			
a. Has a Network Security Officer (NSO) been appointed in writing?			✓
Comments: ______________________________			
b. Have the duties and responsibilities of the NSO been defined in writing?			✓
Comments: ______________________________			

5 JUN 1987

YES NO N/A

c. Do the duties and responsibilities of the NSO include:

(1) Ensuring that countermeasures and security requirements are in the network design and that individual nodes of the network comply with these countermeasures and requirements, prior to interfacing with the network? ✓ ___ ___

Comments: ______________________________

(2) Ensuring that security measures and procedures used at network nodes fully support the security integrity of the network? ✓ ___ ___

Comments: ______________________________

(3) Maintaining liaison with all ADPSSOs in the network? ___ ___ ✓

Comments: ______________________________

(4) Ensuring that all required countermeasuers are utilized? ✓ ___ ___

Comments: ______________________________

14. Are all ADP security violation/incidents reported to the ADPSO? ✓ ___ ___

Comments: ______________________________

15. Do newly assigned ADP personnel receive briefings on:

a. ADP security procedures of the activity ✓ ___ ___

Comments: ______________________________

b. Marking, handling and accountability of classified ADP information? ___ ___ ✓

Comments: ______________________________

5 JUN 1987

	YES	NO	N/A
c. Marking, handling and accountability of ADP sensitive, unclassified information?	✓		

Comments:

	YES	NO	N/A
d. ADP emergency procedures?	✓		

Comments:

SECTION II

SYSTEM

A. **NAME OF SYSTEM:** Z Caps

B. **TYPE OF SYSTEM**

YES NO N/A

1. Office Information System (OIS)

a. Has an Office Information System Security Officer (OISSO) been appointed in writing? X ___ ___

Comments: taso has OISSO responsibilities

b. Have the duties and responsibilities of the OISSO been defined in writing by the ADPSO? X ___ ___

Comments: Same as 1A above

c. Do the duties and responsibilities of the OISSO include: X ___ ___

Comments: Same as 1A above

(1) Being the focal point of all security matters for the OIS systems assigned? X ___ ___

Comments: Same as 1A above

(2) Executing the ADP Security Program as it applies to the assigned OIS systems including preparing and supporting the accreditation support documentation? X ___ ___

Comments: Same as 1A above

(3) Maintaining an inventory of all OIS hardware, system software and major functional appplication systems? X ___ ___

Comments: ___

		YES	NO	N/A
(4)	Monitoring system activity (e.g., identification of the levels and types of data handled by the OIS systems, assignment of passwords, review of audit trails, etc.) to ensure compliance with security directives and procedures?	X	___	___
Comments:	________________			
(5)	Maintaining liaison with remote facilities served by the OIS systems to ensure compliance with applicable security requirements?	___	___	X
Comments:	________________			
(6)	Conducting and documenting risk assessments for the assigned OIS systems?	X	___	___
Comments:	________________			
(7)	Supervising, testing and monitoring, as appropriate, changes in the OIS system affecting the ADP activity posture?	X	___	___
Comments:	________________			
(8)	Implementing appropriate countermeasures required by directive or determined cost effective?	X	___	___
Comments:	________________			
(9)	Assisting the ADPSO in implementing a comprehensive Activity ADP Security Program?	X	___	___
Comments:	________________			
(10)	Developing and testing annual contingency plans for the assigned OIS systems?	X	___	___
Comments:	________________			

	YES	NO	N/A
(11) Monitoring OIS procurements for security impact to ensure compliance with security regulations and known security requirements for the assigned OIS systems?	___	___	X
Comments: ______________________			
d. If the OIS system has remote terminals:			
(1) Have TASOs been appointed?	___	___	X
Comments: ______________________			
(2) Have the duties and responsibilities of the TASOs been defined in writing?	X	___	___
Comments: ______________________			
(3) Do the duties and responsibilities of the TASO include:			
(a) Serving as a single point of contact at his terminal area for the OISSO?	X	___	___
Comments: ______________________			
(b) Implementing and enforcing all security requirements established by the OISSO for remote terminal areas?	X	___	___
Comments: ______________________			
(c) Ensuring all countermeasures for remote terminal areas are in place?	X	___	___
Comments: ______________________			
(d) Developing terminal security procedures for OISSO approval?	X	___	___
Comments: ______________________			

	YES	NO	N/A
(e) Maintaining a current access list of remote devices?			X
Comments:			
(f) Reporting security abnormalities to the OISSO or his designated representative?	X		
Comments:			
(g) Returning to the OISSO products that cannot be identified or which contain extraneous data?	X		
Comments:			
(4) Have security requirements been agreed to in writing between the host site and remote device sites?			X
Comments:			
2. ADP System			
a. Has an ADP System Security Officer (ADPSSO) been appointed in writing?	X		
Comments:			
b. Have the duties and responsibilities of the ADPSSO been defined in writing?	X		
Comments:			
c. Do the duties and responsibilities of the ADPSSO include:			
(1) Being the focal point for all security matters for the ADP systems assigned?	X		
Comments:			

	YES	NO	N/A
(2) Executing the ADP Security Program as it applies to the assigned ADP systems including preparing and supporting the accreditation support documentation?	✓		
Comments:			
(3) Maintaining an inventory of all hardware, system software and major functional application systems?	✓		
Comments:			
(4) Monitoring system activity (e.g., identification of the levels and types of data handled by the ADP systems, assignment of passwords, review of audit trails, etc.) to ensure compliance with security directives and procedures?	✓		
Comments:			
(5) Maintaining liaison with remote facilities served by the ADP systems to ensure compliance with applicable security requirements?			✓
Comments:			
(6) Maintaining liaison with remote facilities served by the ADP system to ensure that a terminal area security officer (TASO) is designated by the served activity where applicable?			✓
Comments:			
(7) Conducting and documenting risk assessments for the assigned ADP systems?	✓		
Comments:			

	YES	NO	N/A
(8) Supervising, testing and monitoring, as appropriate, changes in the ADP system affecting the ADP activity posture?	X	___	___

Comments:____

	YES	NO	N/A
(9) Implementing appropriate countermeasures required by directive or determined cost effective?	X	___	___

Comments:____

	YES	NO	N/A
(10) Assisting the ADPSO in implementing a comprehensive Activity ADP Security Program?	X	___	___

Comments:____

	YES	NO	N/A
(11) Developing and testing annual contingency plans for the assigned ADP systems?	X	___	___

Comments:____

	YES	NO	N/A
(12) Monitoring ADP procurements for security impact to ensure compliance with security regulations and known security requirements for the assigned ADP systems?	X	___	___

Comments:____

d. If the ADP system is a node of a network:

	YES	NO	N/A
(1) Have security requirements been agreed to in writing by the network DAA and the ADP facility DAA of the network?	___	___	X

Comments:____

	YES	NO	N/A
(2) Has an ADPSO been appointed in writing for the node?	___	___	X

Comments:____

	YES	NO	N/A
e. If the ADP system has remote terminals:			
(1) Have Terminal Area Security Officers (TASOs) been appointed?	___	___	X
Comments: ____________________			
(2) Have the duties and responsibilities of the TASOs been defined in writing?	___	___	X
Comments: ____________________			
(3) Do the duties and responsibilities of the TASO include:			
(a) Serving as a single point of contact at his terminal area for the ADPSSO?	___	___	X
Comments: ____________________			
(b) Implementing and enforcing all security requirements established by the ADPSSO for remote terminal areas?	___	___	X
Comments: ____________________			
(c) Ensuring all countermeasures for remote terminal areas are in-place?	___	___	X
Comments: ____________________			
(d) Developing terminal security procedures for ADPSSO approval?	___	___	X
Comments: ____________________			
(e) Maintaining a current access list of remote devices?	___	___	X
Comments: ____________________			
(f) Reporting security abnormalities to the ADPSSO or his designated representive?	___	___	X
Comments: ____________________			

		YES	NO	N/A
(g)	Returning to the ADPSSO ADP products that cannot be identified or which contain extraneous data?	___	___	✓

Comments:____

		YES	NO	N/A
(4)	Have security requirements been agreed to in writing between the host site and remote device sites?	___	___	✓

Comments:____

C. SYSTEM ACCREDITATION YES NO N/A

1. Is this system accounted for on the ADPSO's inventory? [✓ YES] NO N/A

Comments:

2. Has a survey (Figure E-1 in OPNAVINST 5239.1A) been completed on this system? [✓ YES] NO N/A

Comments:

3. Have security operating procedures been developed for this system? [✓ YES] NO N/A

Comments:

4. Has the DAA determined if a risk assessment is required? YES NO [✓ N/A]

Comments:

5. If a risk assessment is required:

a. Has the risk assessment been performed? YES NO [✓ N/A]

Comments:

b. Do the ADPSO and ADPSSO maintain a copy of the risk assessment? [✓ YES] NO N/A

Comments:

c. Is the risk assessment kept updated and repeated:

(1) At least every 5 years? [✓ YES] NO N/A

Comments:

(2) When any change is made to the facility, ADP equipment, system software or application software which effects the overall ADP security posture? [✓ YES] NO N/A

Comments:

	YES	NO	N/A
(3) When any change is made in operational configuration, data sensitivity, or classification level?	✓		

Comments: ______________________________

	YES	NO	N/A
(4) When any change is made which appears to invalidate the original conditions of accreditation?	✓		

Comments: ______________________________

	YES	NO	N/A
6. Has a Security Test and Evaluation (ST&E) been prepared (only for systems processing Level I or II data) which is sufficiently comprehensive to ensure thorough examination and exercising of the system's security control features and procedures and/or in combination, to determine their effectiveness and reliability?	✓		

Comments: ______________________________

	YES	NO	N/A
7. Has an ST&E been performed to determine the effectiveness of countermeasures employed in maintaining the security of the system at an acceptable level of risk?	✓		

Comments: ______________________________

	YES	NO	N/A
8. Do the ADPSO and ADPSSO maintain a copy of the ST&E plan and results?	✓		

Comments: ______________________________

	YES	NO	N/A
9. Is a contingency plan for this system in existence?	✓		

Comments: ______________________________

10. Does the contingency plan, at a minimum, address:

	YES	NO	N/A
a. The actions required to minimize the impact of a fire, flood, civil disorder, natural disaster, or bomb threat?	✓		

Comments: ______________________________

YES NO N/A

b. Backup procedures to conduct essential ADP operational tasks after a disruption to the primary ADP facility? ✓ ___ ___

Comments: ______________________________

c. Recovery procedures to permit rapid restoration of the ADP facility following physical destruction, major damage or loss of data? ✓ ___ ___

Comments: ______________________________

11. Does the contingency operations plan provide for:

a. Local storage of tapes and punched cards in the central computer facility in metal or other fire retardant cabinets? ✓ ___ ___

Comments: ______________________________

b. Duplicate system tapes, startup decks, data base save tapes, and site-unique application program card files or tapes to be maintained in a secure location removed from the central computer facility? ✓ ___ ___

Comments: ______________________________

c. Identification of an alternate site containing compatible equipment? ✓ ___ ___

Comments: ______________________________

d. Destruction or safeguarding of classified material in the central computer facility in the event that the facility must be evacuated? ✓ ___ ___

Comments: ______________________________

12. Has the contingency plan been tested during the past year? ___ ✓ ___

Comments: ______________________________

13. Do the ADPSO and ADPSSO maintain a copy of the Contingency Plan? ✓ ___ ___

Comments: ______________________________

	YES	NO	N/A
14. Do the ADPSO and ADPSSO maintain a copy of the Contingency Plan Test and Evaluation Report?	X	___	___

Comments: ____

D. HUMAN RESOURCES SECURITY

	YES	NO	N/A
1. Do all personnel having unescorted access to the system possess a clearance and a need-to-know equal to or higher than the highest classification and all categories of data being processed?	✓		
Comments:			
2. Is an access roster maintained at each entry point to the central computer facility and remote terminal area?	✓		
Comments:			
3. Are escort procedures established for controlling visitors to the central computer facility and remote terminal areas?	✓		
Comments:			
a. Are all potential escorts properly briefed on their responsibilities?	✓		
Comments:			
b. Is a record of all visitors maintained for 12 months?	✓		
Comments:			
4. During operational hours is the central computer facility manned by at least two cleared personnel?	✓		
Comments:			
5. Are all unescorted maintenance personnel cleared for the highest level and all restrictive categories of classified information in the system?	✓		
Comments:			

	YES	NO	N/A
6. Are escorts provided for maintenance personnel who are not appropriately cleared?	X	___	___

Comments: ______________________________

	YES	NO	N/A
7. Are escorts technically competent to review the maintenance work performed?	___	X	___

Comments: ______________________________

	YES	NO	N/A
8. Are procedures to delete and add personnel to access lists implemented, including the notification of all concerned ADP security officials?	X	___	___

Comments: ______________________________

E. PHYSICAL SECURITY

	YES	NO	N/A
1. Does the computer facility meet the following requirements?			
a. Is the system operated within the manufacturer's optimum temperature and humidity range specifications?	X		
Comments:			
b. Are environmental systems dedicated to the computer facility?		X	
Comments:			
c. Are environmental controls regulated by key designated personnel only?		X	
Comments:			
d. Is a temperature/humidity recording instrument installed to monitor the system area?		X	
Comments:			
(1) Is the temperature/humidity instrument connected to an alarm to warn of near-limit conditions?		X	
Comments:			
e. Is there adequate lighting?	X		
Comments:			
f. Is there emergency lighting?		X	
Comments:			
g. Are periodic checks made of the emergency lighting?		X	
Comments:			

	YES	NO	N/A
h. Is electrical power reliable?	X		
Comments:			
i. Are there voltage regulators or other electronic devices to prevent serious power fluctuations?	X		
Comments:			
j. Is there an uninterruptible power source for the facility?		X	
Comments:			
k. Are cleaning procedures and schedules established and adhered to?	X		
Comments:			
l. Is an ADP representative present during cleaning operations?	X		
Comments:			
m. Is the facility overhead free of steam and water pipes?	X		
Comments:			
n. Are plastic sheets available to protect the system from water damage?	X		
Comments:			
o. Is there a facility fire bill?	X		
Comments:			
p. Are emergency exits clearly marked?	X		
Comments:			
q. Do employees receive periodic training in the following areas:			
(1) Power shut down and start up procedures?	X		
Comments:			

	YES	NO	N/A
(2) Operation of emergency power?	___	___	X
Comments: ______________________			
(3) Operation of fire detection and alarm system?	X	___	___
Comments: ______________________			
(4) Operation of fire suppression equipment?	X	___	___
Comments: ______________________			
(5) Building evacuation procedures?	X	___	___
Comments: ______________________			
r. Is there a master power switch to all ADP equipment?	___	X	___
Comments: ______________________			
s. Is the master power switch located near the main entrance of the ADP area?	___	X	___
Comments: ______________________			
t. Is the master power switch adequately labeled to prevent accidental shut off?	___	___	X
Comments: ______________________			
u. If the system processes critical applications, is there a sequential shut down routine?	___	___	X
Comments: ______________________			
v. Is there a sufficient number of portable fire extinguishers?	X	___	___
Comments: ______________________			

		YES	NO	N/A
w.	Is there a central fire suppression system?		X	
Comments:				
x.	Is there automatic smoke/fire detection equipment?	X		
Comments:				
y.	Does the smoke/fire detection equipment activate an alarm at the nearest fire station?	X		
Comments:				
z.	Are there warning signs posted outside tape vaults and other magnetic storage areas to warn fire fighters of toxic fumes?			X
Comments:				
aa.	If the facility does not operate 24-hours, is there a guard force employed after hours and on weekends?		X	
Comments:				
bb.	Is the guard force briefed on emergency procedures?		X	
Comments:				
cc.	Is the guard force provided with an emergency recall bill?		X	
Comments:				
dd.	Are physical access controls implemented to prevent unauthorized entry into the computer facilities and remote terminal areas?	yes		
Comments:				

		YES	NO	N/A
ee.	Are visitor control procedures in place?	X	___	___

Comments:______________________________

		YES	NO	N/A
ff.	Are positive personnel identification measures (e.g., badge system, fingerprints) in place?	X	___	___

Comments:______________________________

YES NO N/A

F. COMMUNICATIONS SECURITY

1. Do all communications links between remote terminal areas and the central computer facility meet the requirements for the transmission of the highest classification and for all categories of data which are contained in the system? ___ ___ X

Comments:____

2. Are all remote terminals uniquely identified when accessing the host? ___ ___ X

Comments:____

3. Are all dial-up terminals disabled from connection to the central computer facility during classified processing periods? ___ ___ X

Comments:____

YES NO N/A

G. EMANATIONS SECURITY

1. If the ADP system processes Level I data:

a. Has a TEMPEST vulnerability assessment been requested? ___ ___ X

Comments:______________________________

b. Has a TEMPEST vulnerability assessment been performed? ___ ___ X

Comments:______________________________

(1) Does it represent the current equipment configuration? ___ ___ X

Comments:______________________________

c. Are all changes, repairs, and modifications to TEMPEST certified ADPE controlled so that equipment emanation characteristics are not altered? ___ ___ X

Comments:______________________________

H. HARDWARE SECURITY

	YES	NO	N/A
1. Is the site SOP manual used for configuring system hardware?			X
Comments:			
2. Are switch settings for each hardware unit specified for each system?			X
Comments:			
3. Are scheduled maintenance activities monitored to ensure proper reliability and performance?	X		
Comments:			
4. Are periods of down time verified?	X		
Comments:			

I. SOFTWARE SECURITY

	YES	NO	N/A
1. Is the authenticity of the operating system or executive software verified by comparing the registry or shipment number of the software package with that contained in record communications from the originator?	✓		
Comments:			
2. Prior to operational use of any new system release, does the ADPSSO conduct sufficient testing to verify that the system meets the documented and approved security specifications?	✓		
Comments:			
3. Are testing and debugging of new releases performed during dedicated time in a controlled environment?	✓		
Comments:			
4. Are all site-unique patches tested by system software personnel?			✓
Comments:			
5. Is a log of all system patches maintained and monitored by the ADPSSO?			✓
Comments:			
6. Are all modifications to the operating system cross-checked by two appropriately cleared operating system programmers?	✓		
Comments:			
7. Are startup procedures executed as described in the site SOP manual?	✓		
Comments:			

	YES	NO	N/A
8. Are system tapes identified in a unique manner to distinguish them from non-system tapes?	X		
Comments:			
9. Are system tapes protected to the highest classification and for all restrictive categories of data which the central system is processing or storing online?	X		
Comments:			
10. Has a method to control access to system tapes or disks been developed and approved by the ADPSSO?	X		
Comments:			
11. Is the ADPSSO informed of all unauthorized requests for system tape access?	X		
Comments:			
12. Are system module source listings made available to site personnel only on a need-to-know basis and are the listings physically protected as FOUO?	X		
Comments:			
13. Has each individual user been assigned a unique user identification and password which has been randomly, machine generated?	X		
Comments:			
14. Is a password changed:			
a. Whenever an individual knowing a log-on password is transferred, discharged, reassigned or the individual's security clearance is reduced, suspended, or removed by proper authority?	X		
Comments:			

	YES	NO	N/A
b. Whenever a password or record of password has been compromised, or is suspected of being compromised?	X	___	___
Comments: ________________			
c. At least annually?	X	___	___
Comments: ________________			
15. Is removable media controlled at the highest level of data processed and restricted to users cleared for that level?	X	___	___
Comments: ________________			
16. When no longer needed, are data purged or declassified?	X	___	___
Comments: ________________			
17. Does an audit record identify the reason for system shutdown or crash?	X	___	___
Comments: ________________			
18. Are system dumps taken following a system crash?	___	___	X
Comments: ________________			
19. Are system dumps reviewed by the ADPSSO or site analyst?	___	___	X
Comments: ________________			
20. Is all memory purged between periods processing?	___	___	X
Comments: ________________			
21. Are security specifications coordinated by site management prior to approval of application software development and maintenance?	X	___	___
Comments: ________________			

	YES	NO	N/A
22. Are application software design reviews conducted, documented, and maintained as official records of the site?	___	___	X

Comments:

	YES	NO	N/A
23. Are system tests of new application releases conducted?	___	___	X

Comments:

	YES	NO	N/A
24. If operational user files are required for testing, are only copies of the files used?	___	___	X

Comments:

YES NO N/A

J. ADMINISTRATIVE SECURITY

1. Are effective procedures for limiting access to the system and its data established and implemented? X ___ ___

Comments: ______________________________

2. Does the ADPSSO maintain a current roster of all personnel authorized access to the system? X ___ ___

Comments: ______________________________

3. Does the ADPSSO control the distribution of passwords? X ___ ___

Comments: ______________________________

4. Are log-on passwords for unclassified systems marked For Official Use Only (FOUO)? X ___ ___

Comments: ______________________________

5. Are working papers containing classified information marked with:

a. Date of creation? X ___ ___

Comments: ______________________________

b. Highest classification of any information contained in the product? X ___ ___

Comments: ______________________________

6. Are printed listings containing classified information marked with the security classification on the top and bottom of each page? ___ ___ X

Comments: ______________________________

7. Are microfilm and microfiche conspicuously marked on the microform media or its container with the overall security classification so as to be readable with unaided eye? ___ ___ X

Comments: ______________________________

	YES	NO	N/A
8. Are all ADP storage devices externally marked with:			
a. The overall security classification?	X		
Comments:			
b. Special access restrictions?	X		
Comments:			
c. A permanently assigned identification/control number?	X		
Comments:			
9. Do magnetic tapes have a gummed label affixed containing:			
a. Tape classification/declassification?			X
Comments:			
b. Tape identification control number?			X
Comments:			
10. Are removable disk packs marked with the same information required for magnetic tapes?			X
Comments:			
11. Are customers responsible for reviewing and verifying the actual classification of the product?	X		
Comments:			
12. Are effective procedures for protecting personal and other unclassified sensitive data established and implemented?	X		
Comments:			
13. Have procedures for maintaining an inventory of all removable magnetic storage devices been established?		X	
Comments:			

	YES	NO	N/A
14. Is the inventory listing for devices classified TOP SECRET or special category verified at least semiannually?	___	___	X
Comments: ______			
15. Is the inventory listing for devices classified SECRET and below verified at least annually?	___	___	X
Comments: ______			
16. Is magnetic storage media being declassified and disposed of as required by Appendix C of OPNAVINST 5239.1A?	___	___	X
Comments: ______			
17. Are security incidents investigated to determine their cause, and where possible, the corrective action to be taken?	X	___	___
Comments: ______			
18. Are ADP security incidents fully documented and properly reported?	X	___	___
Comments: ______			

PRMIS

ST&E CHECKLIST 5 JUN 1987

SECTION I

ACTIVITY

	YES	NO	N/A
1. Has an ADP Security Program been established?	X		
Comments: ______________________________			
2. Has an Activity ADP Security Plan (AADPSP) been developed?	X		
Comments: ______________________________			
3. Has the AADPSP been approved by the Naval Data Automation Command (NAVDAC) Code 51?	X		
Comments: ______________________________			
4. Has the Designated Approving Authority granted activity accreditation?		X	
Comments: ______________________________			
5. Is the AADPSP updated as changes occur?	X		
Comments: ______________________________			
6. Is there evidence that top-level management supports the ADP Security program through such requirements as security awareness training, documented security procedures, etc.?	X		
Comments: ______________________________			
7. Is the ADP security staff sufficient to support the ADP Security Program?	X		
Comments: ______________________________			

YES NO N/A

8. Has an ADP Security Officer (ADPSO) been appointed in writing by the Commanding Officer? X ___ ___

Comments: ______________________________

9. Does the ADPSO have a strong technical background and experience in the administration of ADP systems? X ___ ___

Comments: ______________________________

10. Has the ADPSO received training on OPNAVINST 5239.1A? X ___ ___

Comments: ______________________________

11. Have the duties and responsibilities of the ADPSO been defined in writing? X ___ ___

Comments: ______________________________

12. Do the duties and responsibilities of the ADPSO include:

a. Coordinating with the command security manager on matters concerning ADP security, in accordance with the security organizational structure established by the Commanding Officer? X ___ ___

Comments: ______________________________

b. Developing and maintaining an ADP Security Plan (ADPSP)? X ___ ___

Comments: ______________________________

c. Ensuring that a Network Security Officer (NSO) is appointed for networks which are sponsored by the activity? X ___ ___

Comments: ______________________________

5 JUN 1987.

	YES	NO	N/A
d. Ensuring that ADP System Security Officers (ADPSSOs) are appointed in writing where applicable?	___	___	X

Comments:____
____

e. Ensuring that Terminal Area Security Officers (TASOs) are appointed where applicable for each remote facility?	X	___	___

Comments:____
____

f. Ensuring that an effective activity Risk Management Program is implemented?	X	___	___

Comments:____
____

g. Ensuring that all ADP security incidents or violations are investigated, documented and reported to appropriate authorities?	X	___	___

Comments:____
____

h. Ensuring that security requirements are included in life cycle management documentation as prescribed in SECNAV Instructions 5000.1A or 5231.1A as appropriate?	X	___	___

Comments:____
____

i. Ensuring that all procurement documents or specifications approved within the activity comply with ADP security requirements?	X	___	___

Comments:____
____

j. Ensuring the contracts (DD Form 254) include statement(s) ensuring contractor compliance with Navy ADP Security requirements?	X	___	___

Comments:____
____

YES NO N/A

k. Ensuring the development and testing of all contingency plans? X ___ ___

Comments: ____________________

l. Ensuring the NAVAUDSVC is advised of the development of an ADP system, as applicable? X ___ ___

Comments: ____________________

m. Ensuring that accreditation documentation is developed and maintained? X ___ ___

Comments: ____________________

n. Assisting the ADP security staff in implementing their respective ADP security requirements? X ___ ___

Comments: ____________________

o. Ensuring that applicable personnel security procedures are established? X ___ ___

Comments: ____________________

p. Ensuring that Security Test and Evaluations (ST&Es) are conducted where applicable? X ___ ___

13. If this activity sponsors a network:

a. Has a Network Security Officer (NSO) been appointed in writing? ___ ___ X

Comments: ____________________

b. Have the duties and responsibilities of the NSO been defined in writing? ___ ___ X

Comments: ____________________

	YES	NO	N/A
c. Do the duties and responsibilities of the NSO include:			
(1) Ensuring that countermeasures and security requirements are in the network design and that individual nodes of the network comply with these countermeasures and requirements, prior to interfacing with the network?	X		
Comments:			
(2) Ensuring that security measures and procedures used at network nodes fully support the security integrity of the network?	X		
Comments:			
(3) Maintaining liaison with all ADPSSOs in the network?			X
Comments:			
(4) Ensuring that all required countermeasuers are utilized?	X		
Comments:			
14. Are all ADP security violation/incidents reported to the ADPSO?	X		
Comments:			
15. Do newly assigned ADP personnel receive briefings on:			
a. ADP security procedures of the activity	X		
Comments:			
b. Marking, handling and accountability of classified ADP information?			X
Comments:			

5 JUN 1987

	YES	NO	N/A
c. Marking, handling and accountability of ADP sensitive, unclassified information?	X	___	___

Comments:____

	YES	NO	N/A
d. ADP emergency procedures?	X	___	___

Comments:____

Prmis

SECTION II

SYSTEM

A. NAME OF SYSTEM: ZENITH 248 (PRMIS)

B. TYPE OF SYSTEM

	YES	NO	N/A
1. Office Information System (OIS)			
a. Has an Office Information System Security Officer (OISSO) been appointed in writing?	X		
Comments: TASO has OISSO responsibilities			
b. Have the duties and responsibilities of the OISSO been defined in writing by the ADPSO?	X		
Comments: Same as 1A above			
c. Do the duties and responsibilities of the OISSO include:	X		
Comments: Same as 1A above			
(1) Being the focal point of all security matters for the OIS systems assigned?	X		
Comments: Same as 1a above			
(2) Executing the ADP Security Program as it applies to the assigned OIS systems including preparing and supporting the accreditation support documentation?	X		
Comments: Same as 1A above			
(3) Maintaining an inventory of all OIS hardware, system software and major functional appplication systems?	X		
Comments:			

		YES	NO	N/A
(4)	Monitoring system activity (e.g., identification of the levels and types of data handled by the OIS systems, assignment of passwords, review of audit trails, etc.) to ensure compliance with security directives and procedures?	X		

Comments:______________________________________

		YES	NO	N/A
(5)	Maintaining liaison with remote facilities served by the OIS systems to ensure compliance with applicable security requirements?			X

Comments:______________________________________

		YES	NO	N/A
(6)	Conducting and documenting risk assessments for the assigned OIS systems?	X		

Comments:______________________________________

		YES	NO	N/A
(7)	Supervising, testing and monitoring, as appropriate, changes in the OIS system affecting the ADP activity posture?	X		

Comments:______________________________________

		YES	NO	N/A
(8)	Implementing appropriate countermeasures required by directive or determined cost effective?	X		

Comments:______________________________________

		YES	NO	N/A
(9)	Assisting the ADPSO in implementing a comprehensive Activity ADP Security Program?	X		

Comments:______________________________________

		YES	NO	N/A
(10)	Developing and testing annual contingency plans for the assigned OIS systems?	X		

Comments:______________________________________

	YES	NO	N/A
(11) Monitoring OIS procurements for security impact to ensure compliance with security regulations and known security requirements for the assigned OIS systems?	___	___	X
Comments: ______			
d. If the OIS system has remote terminals:			
(1) Have TASOs been appointed?	___	___	X
Comments: ______			
(2) Have the duties and responsibilities of the TASOs been defined in writing?	X	___	___
Comments: ______			
(3) Do the duties and responsibilities of the TASO include:			
(a) Serving as a single point of contact at his terminal area for the OISSO?	X	___	___
Comments: ______			
(b) Implementing and enforcing all security requirements established by the OISSO for remote terminal areas?	X	___	___
Comments: ______			
(c) Ensuring all countermeasures for remote terminal areas are in place?	X	___	___
Comments: ______			
(d) Developing terminal security procedures for OISSO approval?	X	___	___
Comments: ______			

	YES	NO	N/A
(e) Maintaining a current access list of remote devices?			X
Comments:			
(f) Reporting security abnormalities to the OISSO or his designated representative?	X		
Comments:			
(g) Returning to the OISSO products that cannot be identified or which contain extraneous data?	X		
Comments:			
(4) Have security requirements been agreed to in writing between the host site and remote device sites?			X
Comments:			
2. ADP System			
a. Has an ADP System Security Officer (ADPSSO) been appointed in writing?	X		
Comments:			
b. Have the duties and responsibilities of the ADPSSO been defined in writing?	X		
Comments:			
c. Do the duties and responsibilities of the ADPSSO include:			
(1) Being the focal point for all security matters for the ADP systems assigned?	X		
Comments:			

	YES	NO	N/A
(2) Executing the ADP Security Program as it applies to the assigned ADP systems including preparing and supporting the accreditation support documentation?	X	___	___

Comments:____

(3) Maintaining an inventory of all hardware, system software and major functional application systems?	X	___	___

Comments:____

(4) Monitoring system activity (e.g., identification of the levels and types of data handled by the ADP systems, assignment of passwords, review of audit trails, etc.) to ensure compliance with security directives and procedures?	X	___	___

Comments:____

(5) Maintaining liaison with remote facilities served by the ADP systems to ensure compliance with applicable security requirements?	___	___	X

Comments:____

(6) Maintaining liaison with remote facilities served by the ADP system to ensure that a terminal area security officer (TASO) is designated by the served activity where applicable?	___	___	X

Comments:____

(7) Conducting and documenting risk assessments for the assigned ADP systems?	X	___	___

Comments:____

	YES	NO	N/A
(8) Supervising, testing and monitoring, as appropriate, changes in the ADP system affecting the ADP activity posture?	X		
Comments:			
(9) Implementing appropriate countermeasures required by directive or determined cost effective?	X		
Comments:			
(10) Assisting the ADPSO in implementing a comprehensive Activity ADP Security Program?	X		
Comments:			
(11) Developing and testing annual contingency plans for the assigned ADP systems?	X		
Comments:			
(12) Monitoring ADP procurements for security impact to ensure compliance with security regulations and known security requirements for the assigned ADP systems?	X		
Comments:			
d. If the ADP system is a node of a network:			
(1) Have security requirements been agreed to in writing by the network DAA and the ADP facility DAA of the network?			X
Comments:			
(2) Has an ADPSO been appointed in writing for the node?			X
Comments:			

YES NO N/A

e. If the ADP system has remote terminals:

(1) Have Terminal Area Security Officers (TASOs) been appointed? ___ ___ X

Comments: ____________________

(2) Have the duties and responsibilities of the TASOs been defined in writing? ___ ___ X

Comments: ____________________

(3) Do the duties and responsibilities of the TASO include:

(a) Serving as a single point of contact at his terminal area for the ADPSSO? ___ ___ X

Comments: ____________________

(b) Implementing and enforcing all security requirements established by the ADPSSO for remote terminal areas? ___ ___ X

Comments: ____________________

(c) Ensuring all countermeasures for remote terminal areas are in-place? ___ ___ X

Comments: ____________________

(d) Developing terminal security procedures for ADPSSO approval? ___ ___ X

Comments: ____________________

(e) Maintaining a current access list of remote devices? ___ ___ X

Comments: ____________________

(f) Reporting security abnormalities to the ADPSSO or his designated representive? ___ ___ X

Comments: ____________________

	YES	NO	N/A
(g) Returning to the ADPSSO ADP products that cannot be identified or which contain extraneous data?	___	___	X

Comments: ______________________________

	YES	NO	N/A
(4) Have security requirements been agreed to in writing between the host site and remote device sites?	___	___	X

Comments: ______________________________

C. SYSTEM ACCREDITATION	YES	NO	N/A
1. Is this system accounted for on the ADPSO's inventory?	X	___	___
Comments: ________________			
2. Has a survey (Figure E-1 in OPNAVINST 5239.1A) been completed on this system?	X	___	___
Comments: ________________			
3. Have security operating procedures been developed for this system?	X	___	___
Comments: ________________			
4. Has the DAA determined if a risk assessment is required?	___	___	X
Comments: ________________			
5. If a risk assessment is required:			
a. Has the risk assessment been performed?	___	___	X
Comments: ________________			
b. Do the ADPSO and ADPSSO maintain a copy of the risk assessment?	X	___	___
Comments: ________________			
c. Is the risk assessment kept updated and repeated:			
(1) At least every 5 years?	X	___	___
Comments: ________________			
(2) When any change is made to the facility, ADP equipment, system software or application software which effects the overall ADP security posture?	X	___	___
Comments: ________________			

	YES	NO	N/A
(3) When any change is made in operational configuration, data sensitivity, or classification level?	X	___	___
Comments: ______________________________			
(4) When any change is made which appears to invalidate the original conditions of accreditation?	X	___	___
Comments: ______________________________			
6. Has a Security Test and Evaluation (ST&E) been prepared (only for systems processing Level I or II data) which is sufficiently comprehensive to ensure thorough examination and exercising of the system's security control features and procedures and/or in combination, to determine their effectiveness and reliability?	X	___	___
Comments: ______________________________			
7. Has an ST&E been performed to determine the effectiveness of countermeasures employed in maintaining the security of the system at an acceptable level of risk?	X	___	___
Comments: ______________________________			
8. Do the ADPSO and ADPSSO maintain a copy of the ST&E plan and results?	X	___	___
Comments: ______________________________			
9. Is a contingency plan for this system in existence?	X	___	___
Comments: ______________________________			
10. Does the contingency plan, at a minimum, address:			
a. The actions required to minimize the impact of a fire, flood, civil disorder, natural disaster, or bomb threat?	X	___	___
Comments: ______________________________			

YES NO N/A

b. Backup procedures to conduct essential ADP operational tasks after a disruption to the primary ADP facility? X ___ ___

Comments: ______________________________

c. Recovery procedures to permit rapid restoration of the ADP facility following physical destruction, major damage or loss of data? X ___ ___

Comments: ______________________________

11. Does the contingency operations plan provide for:

a. Local storage of tapes and punched cards in the central computer facility in metal or other fire retardant cabinets? X ___ ___

Comments: ______________________________

b. Duplicate system tapes, startup decks, data base save tapes, and site-unique application program card files or tapes to be maintained in a secure location removed from the central computer facility? X ___ ___

Comments: ______________________________

c. Identification of an alternate site containing compatible equipment? X ___ ___

Comments: ______________________________

d. Destruction or safeguarding of classified material in the central computer facility in the event that the facility must be evacuated? X ___ ___

Comments: ______________________________

12. Has the contingency plan been tested during the past year? ___ X ___

Comments: ______________________________

13. Do the ADPSO and ADPSSO maintain a copy of the Contingency Plan? X ___ ___

Comments: ______________________________

	YES	NO	N/A
14. Do the ADPSO and ADPSSO maintain a copy of the Contingency Plan Test and Evaluation Report?	X		

Comments:

	YES	NO	N/A
D. HUMAN RESOURCES SECURITY			
1. Do all personnel having unescorted access to the system possess a clearance and a need-to-know equal to or higher than the highest classification and all categories of data being processed?	X	___	___
Comments:______			
2. Is an access roster maintained at each entry point to the central computer facility and remote terminal area?	X	___	___
Comments:______			
3. Are escort procedures established for controlling visitors to the central computer facility and remote terminal areas?	X	___	___
Comments:______			
a. Are all potential escorts properly briefed on their responsibilities?	X	___	___
Comments:______			
b. Is a record of all visitors maintained for 12 months?	X	___	___
Comments:______			
4. During operational hours is the central computer facility manned by at least two cleared personnel?	X	___	___
Comments:______			
5. Are all unescorted maintenance personnel cleared for the highest level and all restrictive categories of classified information in the system?	X	___	___
Comments:______			

	YES	NO	N/A
6. Are escorts provided for maintenance personnel who are not appropriately cleared?	X	___	___
Comments: ______________________________			
7. Are escorts technically competent to review the maintenance work performed?	___	X	___
Comments: ______________________________			
8. Are procedures to delete and add personnel to access lists implemented, including the notification of all concerned ADP security officials?	X	___	___
Comments: ______________________________			

E. PHYSICAL SECURITY

	YES	NO	N/A
1. Does the computer facility meet the following requirements?			
a. Is the system operated within the manufacturer's optimum temperature and humidity range specifications?	X		
Comments:			
b. Are environmental systems dedicated to the computer facility?		X	
Comments:			
c. Are environmental controls regulated by key designated personnel only?		X	
Comments:			
d. Is a temperature/humidity recording instrument installed to monitor the system area?		X	
Comments:			
(1) Is the temperature/humidity instrument connected to an alarm to warn of near-limit conditions?		X	
Comments:			
e. Is there adequate lighting?	X		
Comments:			
f. Is there emergency lighting?		X	
Comments:			
g. Are periodic checks made of the emergency lighting?		X	
Comments:			

		YES	NO	N/A
h.	Is electrical power reliable?	X		
Comments:				
i.	Are there voltage regulators or other electronic devices to prevent serious power fluctuations?	X		
Comments:				
j.	Is there an uninterruptible power source for the facility?		X	
Comments:				
k.	Are cleaning procedures and schedules established and adhered to?	X		
Comments:				
l.	Is an ADP representative present during cleaning operations?	X		
Comments:				
m.	Is the facility overhead free of steam and water pipes?	X		
Comments:				
n.	Are plastic sheets available to protect the system from water damage?	X		
Comments:				
o.	Is there a facility fire bill?	X		
Comments:				
p.	Are emergency exits clearly marked?	X		
Comments:				
q.	Do employees receive periodic training in the following areas:			
	(1) Power shut down and start up procedures?	X		
Comments:				

		YES	NO	N/A
(2)	Operation of emergency power?			X
Comments:				
(3)	Operation of fire detection and alarm system?	X		
Comments:				
(4)	Operation of fire suppression equipment?	X		
Comments:				
(5)	Building evacuation procedures?	X		
Comments:				
r.	Is there a master power switch to all ADP equipment?		X	
Comments:				
s.	Is the master power switch located near the main entrance of the ADP area?		X	
Comments:				
t.	Is the master power switch adequately labeled to prevent accidental shut off?			X
Comments:				
u.	If the system processes critical applications, is there a sequential shut down routine?			X
Comments:				
v.	Is there a sufficient number of portable fire extinguishers?	X		
Comments:				

		YES	NO	N/A
w.	Is there a central fire suppression system?		X	
Comments:				
x.	Is there automatic smoke/fire detection equipment?	X		
Comments:				
y.	Does the smoke/fire detection equipment activate an alarm at the nearest fire station?	X		
Comments:				
z.	Are there warning signs posted outside tape vaults and other magnetic storage areas to warn fire fighters of toxic fumes?			X
Comments:				
aa.	If the facility does not operate 24-hours, is there a guard force employed after hours and on weekends?		X	
Comments:				
bb.	Is the guard force briefed on emergency procedures?		X	
Comments:				
cc.	Is the guard force provided with an emergency recall bill?		X	
Comments:				
dd.	Are physical access controls implemented to prevent unauthorized entry into the computer facilities and remote terminal areas?	yes		
Comments:				

9

		YES	NO	N/A
ee.	Are visitor control procedures in place?	X	___	___

Comments: ______________________________

		YES	NO	N/A
ff.	Are positive personnel identification measures (e.g., badge system, fingerprints) in place?	X	___	___

Comments: ______________________________

YES NO N/A

F. COMMUNICATIONS SECURITY

1. Do all communications links between remote terminal areas and the central computer facility meet the requirements for the transmission of the highest classification and for all categories of data which are contained in the system? ___ ___ X

Comments: ____________________________________

2. Are all remote terminals uniquely identified when accessing the host? ___ ___ X

Comments: ____________________________________

3. Are all dial-up terminals disabled from connection to the central computer facility during classified processing periods? ___ ___ X

Comments: ____________________________________

	YES	NO	N/A
G. EMANATIONS SECURITY			
1. If the ADP system processes Level I data:			
a. Has a TEMPEST vulnerability assessment been requested?	___	___	X
Comments:______			
b. Has a TEMPEST vulnerability assessment been performed?	___	___	X
Comments:______			
(1) Does it represent the current equipment configuration?	___	___	X
Comments:______			
c. Are all changes, repairs, and modifications to TEMPEST certified ADPE controlled so that equipment emanation characteristics are not altered?	___	___	X
Comments:______			

H. HARDWARE SECURITY

	YES	NO	N/A
1. Is the site SOP manual used for configuring system hardware?			X
Comments:			
2. Are switch settings for each hardware unit specified for each system?			X
Comments:			
3. Are scheduled maintenance activities monitored to ensure proper reliability and performance?	X		
Comments:			
4. Are periods of down time verified?	X		
Comments:			

	YES	NO	N/A
I. **SOFTWARE SECURITY**			
1. Is the authenticity of the operating system or executive software verified by comparing the registry or shipment number of the software package with that contained in record communications from the originator?	X		
Comments:			
2. Prior to operational use of any new system release, does the ADPSSO conduct sufficient testing to verify that the system meets the documented and approved security specifications?	X		
Comments:			
3. Are testing and debugging of new releases performed during dedicated time in a controlled environment?	X		
Comments:			
4. Are all site-unique patches tested by system software personnel?			X
Comments:			
5. Is a log of all system patches maintained and monitored by the ADPSSO?			X
Comments:			
6. Are all modifications to the operating system cross-checked by two appropriately cleared operating system programmers?	X		
Comments:			
7. Are startup procedures executed as described in the site SOP manual?	X		
Comments:			

	YES	NO	N/A
8. Are system tapes identified in a unique manner to distinguish them from non-system tapes?	X		
Comments:			
9. Are system tapes protected to the highest classification and for all restrictive categories of data which the central system is processing or storing online?	X		
Comments:			
10. Has a method to control access to system tapes or disks been developed and approved by the ADPSSO?	X		
Comments:			
11. Is the ADPSSO informed of all unauthorized requests for system tape access?	X		
Comments:			
12. Are system module source listings made available to site personnel only on a need-to-know basis and are the listings physically protected as FOUO?	X		
Comments:			
13. Has each individual user been assigned a unique user identification and password which has been randomly, machine generated?	X		
Comments:			
14. Is a password changed:			
a. Whenever an individual knowing a log-on password is transferred, discharged, reassigned or the individual's security clearance is reduced, suspended, or removed by proper authority?	X		
Comments:			

	YES	NO	N/A
b. Whenever a password or record of password has been compromised, or is suspected of being compromised?	X		
Comments:			
c. At least annually?	X		
Comments:			
15. Is removable media controlled at the highest level of data processed and restricted to users cleared for that level?	X		
Comments:			
16. When no longer needed, are data purged or declassified?	X		
Comments:			
17. Does an audit record identify the reason for system shutdown or crash?	X		
Comments:			
18. Are system dumps taken following a system crash?			X
Comments:			
19. Are system dumps reviewed by the ADPSSO or site analyst?			X
Comments:			
20. Is all memory purged between periods processing?			X
Comments:			
21. Are security specifications coordinated by site management prior to approval of application software development and maintenance?	X		
Comments:			

	YES	NO	N/A
22. Are application software design reviews conducted, documented, and maintained as official records of the site?			X
Comments:			
23. Are system tests of new application releases conducted?			X
Comments:			
24. If operational user files are required for testing, are only copies of the files used?			X
Comments:			

J. ADMINISTRATIVE SECURITY

	YES	NO	N/A
1. Are effective procedures for limiting access to the system and its data established and implemented?	X		
Comments:			
2. Does the ADPSSO maintain a current roster of all personnel authorized access to the system?	X		
Comments:			
3. Does the ADPSSO control the distribution of passwords?	X		
Comments:			
4. Are log-on passwords for unclassified systems marked For Official Use Only (FOUO)?	X		
Comments:			
5. Are working papers containing classified information marked with:			
a. Date of creation?	X		
Comments:			
b. Highest classification of any information contained in the product?	X		
Comments:			
6. Are printed listings containing classified information marked with the security classification on the top and bottom of each page?			X
Comments:			
7. Are microfilm and microfiche conspicuously marked on the microform media or its container with the overall security classification so as to be readable with unaided eye?			X
Comments:			

	YES	NO	N/A
8. Are all ADP storage devices externally marked with:			
a. The overall security classification?	X		
Comments:			
b. Special access restrictions?	X		
Comments:			
c. A permanently assigned identification/control number?	X		
Comments:			
9. Do magnetic tapes have a gummed label affixed containing:			
a. Tape classification/declassification?			X
Comments:			
b. Tape identification control number?			X
Comments:			
10. Are removable disk packs marked with the same information required for magnetic tapes?			X
Comments:			
11. Are customers responsible for reviewing and verifying the actual classification of the product?	X		
Comments:			
12. Are effective procedures for protecting personal and other unclassified sensitive data established and implemented?	X		
Comments:			
13. Have procedures for maintaining an inventory of all removable magnetic storage devices been established?		X	
Comments:			

	YES	NO	N/A
14. Is the inventory listing for devices classified TOP SECRET or special category verified at least semiannually?	___	___	X
Comments: ________________________________			
15. Is the inventory listing for devices classified SECRET and below verified at least annually?	___	___	X
Comments: ________________________________			
16. Is magnetic storage media being declassified and disposed of as required by Appendix C of OPNAVINST 5239.1A?	___	___	___
Comments: ________________________________			
17. Are security incidents investigated to determine their cause, and where possible, the corrective action to be taken?	X	___	___
Comments: ________________________________			
18. Are ADP security incidents fully documented and properly reported?	X	___	___
Comments: ________________________________			

AUTHORIZED PERSONNEL ACCESS LIST

AUTHORIZED TERMINAL USERS ACCESS LIST

System: PRMIS

Date: 6-25-92

NAME	JOB TITLE
Sylvia S. Koss	Printing Clerk
ANN R. Horning	Office clerk (OA)

Additional Comments

unauthorized use to be reported to TASO.

Attachment (B) to
Enclosure (7)

AUTHORIZED PERSONNEL ACCESS LIST

AUTHORIZED TERMINAL USERS ACCESS LIST

System: Z-Caps

Date: 6-25-95

NAME	JOB TITLE
R. L. Nueberger	Press foreman SupvR
L.C. Bradley	Printing Officer
S.S. Koss	Printing Clerk
G. D. Pierce	Photographer

Additional Comments

Attachment (B) to
Enclosure (7)

SOFTWARE COPYRIGHT AGREEMENT

I hereby agree to abide by all applicable copy right restrictions placed on all software I will use in a business capacity. I am aware that this applies to the duplication, distribution, and proper control of all software. I am alsoaware that this agreement applies to all Government-owned software.

NAME	SIGNATURE	DATE
ROBERT L. NIEBERGER	Robert L. Nieberger	7/14/93
GEORGE D. PIERCE	George D. Pierce	7/14/93
SYLVIA S. KOSS	Sylvia S. Koss	7/14/93
ANN R. HORNING	Ann R Horning	7/14/93
LEROY C. BRADLEY	LeRoy C. Bradley	7/14/93

ASSET VALUATION WORKSHEET

1. ASSET NAME

Zcaps

2. ASSET DESCRIPTION AND JUSTIFICATION OF IMPACT VALUE RATINGS ASSIGNED.

Hardware

One Z-248 microcomputer with 20 MB hard Disk Drive & One Floppy disk drive w/ color monitor. $2,400.00

Epsom Printer FX 286 $300.00

Spurge Protection Sprit 4.95

total asset Value 2,204.95

Data

Utilizing the impact category of Disclosure resulted in the highest impact Value.

Disclosure level II Data Was assigned a Value of $1,0,000 (table E-2 of OpNavinst 5239.1A)

total asset Value $10,000.00

3. IMPACT VALUE RATING BY IMPACT AREA

□ MODIFICATION □ DESTRUCTION □ DISCLOSURE □ DENIAL OF SERVICE

ASSET VALUATION WORKSHEET

1. ASSET NAME

Zcaps

2. ASSET DESCRIPTION AND JUSTIFICATION OF IMPACT VALUE RATINGS ASSIGNED.

Software

Utilizing the Impact category of destruction resulted in the Highest impact Value. The Valuation of hardware assets consist of the total replacement cost of the operating & Application Software & the time required to restore System.

Cost to replace Software	356.28
Six hours estimated for a GS-3, clerk typist to restore System (13515 divided by 2087 X 1.38)	53.52

total Asset Value: $409.80

Personnel

Utilizing the Impact Category of denial of Service due to System failure/System Shutdown resulted in the highest Impact Value. Duration of such instances is estimated to be 8 hr each, 4 times per year. The Value of this asset is based on personnel whose duties are related Specifically to the operation of the Zcaps computer. The Asset is Valued as follows:

3. IMPACT VALUE RATING BY IMPACT AREA

□ MODIFICATION □ DESTRUCTION □ DISCLOSURE □ DENIAL OF SERVICE

ASSET VALUATION WORKSHEET

1. ASSET NAME

ZCaps

2. ASSET DESCRIPTION AND JUSTIFICATION OF IMPACT VALUE RATINGS ASSIGNED.

Primary users (hourly salary X 8hrs X 38% X 4)

1- GS-4 Printing clerk	108.22
1 - WS-10 Shop foreman	255.36
1 - WG-10 Lithographic Process photographer	196.01
total asset Value	$559.59

3. IMPACT VALUE RATING BY IMPACT AREA

□ MODIFICATION □ DESTRUCTION □ DISCLOSURE □ DENIAL OF SERVICE

ADP SECURITY SURVEY

SECTION I. Basic Data. (Applies to all ADP systems, networks, and OISs)

1. System Identification: Pimis

( ) Office Information System

☒ ADP System

( ) Network

2. System Description: (List all components, main frames, peripherals, communications processors, encryption devices, remote devices, network and remote interfaces, etc.)

One Z-248 microcomputer w/20 MB
Hard Drive & One floppy Disk Drive,
One Hayes modem, One MPI 180
FT Printer

FIGURE E-1 (Page 1 of 10)

ADP SECURITY SURVEY

3. Equipment Location: Bldg 80, Camp Lejeune, N.C.

4. System Operations Contact for Security:

Name: Sylvia J. Koss Code: ____________

Bldg: 80 Room: ________ Phone: AU-484-5919/5131

5. Types of Data Processed and Security Modes of Operation

TYPE OF DATA	PERCENT OF PROCESSING TIME	SECURITY MODE OF OPERATION*
Level I		
SCI		
SIOP-ESI		
TOP SECRET		
SECRET		
CONFIDENTIAL		
Level II		
Privacy Act	10%	Limited Access
For Official Use Only	20%	" "
Financial	70%	" "
Sensitive Management		
Proprietary		
Privileged		
Level III		
TOTAL	100%	

(Note: Applicable security modes are: Compartmented, Controlled, Dedicated, System High, Multilevel, Limited Access, as defined in Appendix A of this manual.)

FIGURE E-1 (Page 2 of 10)

ADP SECURITY SURVEY

6. Operating System and Standard Applications Software Identifications:

____

____

____

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

(✓) Stand-alone and single controlled area (single CPU with single workstation).

( ) Shared logic and single controlled area (single CPU with multiple workstations).

( ) Shared logic and more than one controlled area (single CPU with multiple workstations).

( ) Multiple processors and single controlled area (multiple CPUs).

( ) Multiple processors and more than one controlled area (multiple CPUs).

( ) Used with a remote computer __________ percent of time.

( ) Other: ____

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

A. Equipment: $ _______________

B. Software: $ _______________

C. Data: $ _______________
(Note: Dollar values in Table E-2 can be used as a guideline for computing value of data files.)

ADP SECURITY SURVEY

9. Mission Relatedness

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 ADP function.) Provide justification.

Section II. Site Security Profile and Minimum Requirements for Environmental and Physical Security. (Applies to all ADP systems, networks, and OISs.)

1. Vulnerability: Temperature or Humidity Outside Normal Range.

Operating Countermeasures: (Check all that apply.)

(✓) Adequate heating and controls
(✓) Adequate cooling and controls
(✓) Only designated personnel operate controls
( ) Functioning temperature and humidity recorder
( ) Functioning temperature/humidity warning system
( ) Other: ________________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

FIGURE E-1 (Page 4 of 10)

ADP SECURITY SURVEY

2. Vulnerability: Inadequate Lighting or Electrical Service.

Operating Countermeasures: (Check all that apply.)

(✓) Adequate primary lighting
(✓) Adequate emergency lighting
(✓) Adequate periodic checks of emergency lighting
(✓) Adequate primary power and outlets
( ) Functioning power filters or voltage regulators
( ) Available backup power
( ) Other: ______________________________

Assessment of Risk:

( ) High (✓) Moderate ( ) Low

3. Vulnerability: Improper Housekeeping.

Operating Countermeasures: (Check all that apply.)

(✓) Routine cleaning schedule is adhered to
(✓) Cleaning personnel are trained in computer room procedures
(✓) An ADP facility representative is present during cleaning
(✓) Dust contributors are not permitted in equipment areas (outer coats, throw rugs, drapes, venetian blinds, etc.)
(✓) Air-conditioning filters are cleaned/replaced regularly
( ) Floors are polished with non-flake wax using proper buffer materials or properly damp-mopped
(✓) Carpet areas are vacuumed frequently and anti-static spray is used regularly
(✓) Smoking, eating, and drinking are not permitted in equipment areas
( ) Other: ______________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

ADP SECURITY SURVEY

4. Threat: Water Damage.

Operating Countermeasures: (Check all that apply.)

(✓) Water/steam pipes are not located above equipment
( ) Water/steam pipes are inspected at regular intervals
( ) Functioning humidity warning system
( ) Dry-pipe sprinkler system
( ) Raised floor
(✓) Plastic sheets available to cover susceptible equipment
( ) Water detection devices
( ) Other: ______________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

5. Threat: Fire.

Operating Countermeasures: (Check all that apply.)

(✓) Up-to-date fire bill posted
(✓) Periodic fire drills
(✓) Training--fire prevention methods
(✓) Training--emergency power down procedures
(✓) Trainng--knowledge of fire detection system
(✓) Training--use of fire extinguishers
(✓) Training--use of fire alarm system
(✓) Training--evacuation plan
(✓) Training--individual responsibilities in case of fire
(✓) Functioning emergency power-off switches
( ) Sprinkler system installed
( ) Halon system installed
( ) Carbon dioxide fire extinguishers installed
(✓) Smoke/heat detectors installed
(✓) Functioning fire alarm system
(✓) Emergency exits clearly marked
( ) Other: ______________________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

ADP SECURITY SURVEY

6. Vulnerability: Unauthorized Physical Access.

Operating Countermeasures: (Check all that apply.)

(✓) Perimeter fence
(✓) Security guards
(✓) Building secured outside of normal working hours
( ) Area alarms (motion detectors, open door detectors, perimeter penetration detectors)
(✓) Authorized access list
( ) Cypher door lock
( ) Combination door lock
(✓) Recognition of authorized personnel
( ) Closed circuit television
(✓) Administrative procedures
( ) Physical isolation/protection
( ) High employee morale
(✓) Close supervision of employees
(✓) Indoctrination of personnel in security awareness
( ) Other: ____________________

Assessment of Risk:

( ) High ( ) Moderate (✓) Low

SECTION III. Current status of accreditation support documentation. (Applies to all ADP activities and networks which will be authorized to handle Level I or Level II data.)

1. All ADP activities and networks which will be authorized to handle Level I or II data must either be accredited or be granted interim authority to operate pending accreditation. Accreditation is based on supporting documentation including a risk assessment. This section provides a statement of the current status of the accreditation support documentation. (Check all that apply.)

FIGURE E-1 (PAGE 7 of 10)

ADP SECURITY SURVEY

________________ In existence
______________ Being developed
__________ Required but no action taken
______ Not required

(✓) ( ) ( ) ( ) Security Operating Procedures Handbook

( ) ( ) ( ) (✓) Line diagrams showing interconnection of components and physical layout

(✓) ( ) ( ) ( ) Description of countermeasures in place

(✓) ( ) ( ) ( ) Copies of previous accreditation or interim authority to operate

( ) ( ) ( ) (✓) TEMPEST accreditation request

( ) ( ) ( ) (✓) TEMPEST accreditation test results

(✓) ( ) ( ) ( ) Physical accreditation

(✓) ( ) ( ) ( ) ST&E Test Plan

(✓) ( ) ( ) ( ) Contingency Plan

(✓) ( ) ( ) ( ) Contingency Plan test results

(✓) ( ) ( ) ( ) Formal Risk Assessment

( ) ( ) ( ) ( ) Other (specify): ______________________

SECTION IV. Countermeasure Documentation for Office Information Systems. (Applies to all OISs which will be authorized to handle Level I or Level II.)

1. OISs Handling Level II Data. (Check all that apply.)

( ) The OIS will be authorized to handle Level II data. A list of the operating countermeasures is attached. These countermeasures provide proper data protection and audit trails.

( ) The OIS is a shared logic system with more than one simultaneous user not having need-to-know for all data within the system. Password protection or other equivalent countermeasures are employed for system access and for individual file access.

( ) The OIS Security Operating Procedures have been documented and approved.

ADP SECURITY SURVEY

2. OISs handling Level I Data. (Check all that apply.)

( ) The OIS will be authorized to handle Level I data under a system high or dedicated mode of operation. A list of the operating countermeasures is attached. These countermeasures satisfy security requirements.

( ) TEMPEST accreditation has been requested. Request date __________.

( ) TEMPEST accreditation has been received. Accreditation date __________.

( ) The OIS Security Operating Procedures have been documented and approved.

SECTION V. Survey Data. (Applies to all ADP systems, networks, or OISs.)

1. Current Status: (Check all that apply.)

( ) Operating under accreditation for processing Level __________ data in __________ security mode of operation. Accreditation granted by _______________. Dated __________. (Attach a copy of statement of accreditation.)

( ) Operating under interim authority for processing Level __________ data in __________ security mode of operation. Interim authority granted by _______________. Dated __________. Expires __________. (Attach a copy of interim authority to operate.)

2. Survey Prepared By:

Name:____________________________ Code:_________________

Bldg:__________ Room: __________ Phone:_________________

FIGURE E-1 (Page 9 of 10)

ADP SECURITY SURVEY

To the best of my knowledge, the information provided in this survey and the attached documentation is complete and accurate.

Signature ______________________________ Date _____________

(Provide a list of all survey team members.)

FIGURE E-1 (Page 10 of 10)

CONTINGENCY PLAN

PLAN INTRODUCTION

1. INTRODUCTION

1.1 PURPOSE.

This document establishes and implements the Contingency Plan for the Defense Printing Service Detachment Branch Office ADP/OIS systems. This plan pro-vides essential guidance for contingency preparations, emergency reactions and backup operations following the occurrence of contingency situations.

1.2 OBJECTIVES

Adverse incidents are normally followed by periods of disorientation. The failure to react to contingency situations in a preconceived manner often results in losses greater than those caused by the incident.

Losses following contingency occurrences can be reduced by assessing the operational environment, planning courses of action, assigning responsibilities for those actions, and ensuring that the actions will occur through practice. The accomplishment of these attributes is the central objective of this plan.

1.3 PLANNING CONSIDERATIONS

1.3.1 MISSION

The primary mission of DPSDBO is to provide printing and publications services to the Navy, the Department of Defense and Federal Agencies. Financial management reporting responsibility is to the DPSDO, Charleston, SC. Operational (production) responsibility for printing services is under the authority of the Joint Committee on Printing, Congress of the United States (JCP).

1.3.2 EXISTING PROGRAMMED CAPABILITIES

DPSDBO currently operates an automated pricing system that provides summary pricing schedules and consolidated reports to satisfy the requirements for input documentation which is forwarded to DPSDO, Charleston, SC. Other automated systems currently operational include electronic page printing, automated composition and editing, and systems operated in support of the Navy's reprographic equipment and printing production efforts. OIS systems which handle the processing of Level II and III data are also operational within the DPSDBO to support the DPS charter.

1.3.3 ENVIRONMENTAL ASSESSMENT

In determining the scope of this contingency plan, risk assessments of the DPSDBO systems were used to evaluate the operational environment and resultant contingency requirements.

1.3.4 RISK ASSESSMENT

The risk assessments were completed prior to the development of this plan. Through this process, potential threats and their impact on DPSDBO resources were identified and evaluated. Cost-effective countermeasures have since been identified and are being implemented to minimize possible losses from these threats.

1.3.5 WORKLOAD EVALUATION AND PRIORITIZATION

A primary concern in developing this plan was to carefully arrive at an economic balance between adequate protection and the cost of that protection.

Consideration was given to the fact that DPSDBO currently maintains duplicate systems that can be used in a backup capacity. Other noted systems within the DPSDBO are self-standing special purpose units utilized in support of the printing and publications process which involve no transmission of data. OI systems overall do not utilize any transmission of data and no OI system within DPSDBO is authorized to handle Level I data.

1.3.6 CRITICAL DEPENDENCIES

Potential emergencies anticipated to have a high probability which would cause a disruption of service include hardware failure, data capture disk failure, and operator error. While any reasonable disruption of service would be an annoyance, it would not have a serious impact on the DPSDBO mission.

1.4 PLANNING ASSUMPTIONS

This plan is based upon the current workload, procedures, and capabilities of the DPSDBO systems. To establish and maintain a planning base, the following assumptions were drawn and used in the development of this plan.

The current risk assessments considered all of the potential treats that should be accounted for, reflect accurately calculated annual loss expectancies (ALEs), and properly indicate residual risk.

Subsequent risk assessments will be conducted at the frequency required by the Department of the Navy ADP Security Program.
This plan will be validated against the results of future risk

assessments to ensure its continuing currency.

The procedures provided in this plan will be kept current with the capabilities of DPSDBO systems.

Where necessary, backup copies of system software, applications systems, program files, data files and all supporting documentation is maintained off-site in a manner that will allow necessary retrieval of same.

This plan will be tested annually as required by Department of the Navy ADP Security policy.

1.5. STRUCTURE OF THE PLAN

Part I of the plan contains those preparatory actions necessary to ensure rapid implementation of the remainder of the plan. Items detailed in this section include requirements to establish and maintain application backups and the training of all system personnel.

Part II of the plan specifies actions to be taken to ensure continuity of operations following a reduction or loss of local processing capability and contains the procedures to follow when a component's capability has been reduced or a system is unavailable for extended periods of time. Included is an identification of alternative processing sites.

PART I

2. CONTINGENCY PREPARATION

During the planning process, it was determined that the readiness of DPSDBO facilities to respond to an ADP/OI contingency situation is dependent upon the currency of such essential information as the requirements for a backup processing capability, personnel training and the identification of which personnel are to be trained in contingency situations.

2.1 APPLICATION BACKUP

The ability to continue operations after a contingency situation occurs, is largely dependent upon ensuring that applications software survives the emergency. For this reason, a primary thrust of contingency preparation is to ensure the survival of important software. For each application, the need to backup individual programs, data and documentation depends in part on how these items were obtained originally.

In determining the software backup requirements for DPSDBO systems, it was obvious that all locally produced software must be backed up locally. Software obtained from outside sources need only be backed up locally if additional copies cannot be obtained from outside sources within a reasonable time.

Backup requirements have been identified for applications processed by DPSDBO systems and have been incorporated into the daily procedures as follows:

Backups of any programs will be made after any new receipt/change.

Backups of data will be made following each update of a data file, or at the end of each work day.

Additionally, two copies of program software and data files which are not retrievable through DPSMO Washington, vendor support, or other DPSDBO components are produced to support this plan. One copy is used as a working copy to accomplish normal processing. A second, "on-site backup" copy is stored in a fireproof container away from the processing site. The original program software, where possible and feasible, will be stored at an off site location.

2.2 CONTINGENCY REACTION PERSONNEL

From an economic view, it is unrealistic to expect to be able to train all personnel to respond appropriately when processing contingencies arise. At the same time, key DPSDBO personnel must be ready to respond to these situations with minimal delay and acceptable proficiency. The DPSDBO TASO will be cognizant of all contingency requirements.

2.3 CONTINGENCY PLAN TESTING

This plan will be tested initially, and at least annually thereafter. Future tests will simulate operational scenarios and will be conducted and documented as required.

PART II
CONTINGENCY REACTION PLAN

3. PROCEDURES GOVERNING DPSDBO SYSTEMS

In the event that the automated data proeessing capability at DPSDBO is incapacitated for a period in excess of ten working days, it will be brought to the attention of the DPS SOEASTAREA ADP Security Officer (ADPSO), his/her alternative or the Security Manager.

The ADPSO will coordinate equipment and personnel logistics as required, and maintain a log of equipment relocations.

3.1 FINANCIAL SYSTEM

DPS automatic data processing support for the Financial System is furnished by the U. S. Department of Agriculture (USDA) via an interagency agreement. The USDA acts as an ADP Service Center for DPS and other users of their systems. They provide on a reimbursable basis for telecommunications services, the housing of applications and system software, transmitted data and for processing DPS' data.

The USDA contracts with the Department of Transportation (DOT) for the provision of alternate site processing of its users applications in emergency situations. The USDA and DOT have a similar configuration of ADP support equiument and are capable of supporting each other should an emergency arise. NPPS data files are stored off-site from the data processing center and provisions are incorporated in the DPS interagency agreement for contingency emergency support.

3.2 SUPPLY SYSTEM

DPSBDO program support for the Supply System is provided for locally. In the event that the DPSDBO microcomputer system is inoperative and would remain so for a period of time that would effect the end-of-month reporting the following backup/recovery operations will apply. If a second microcomputer where the supply system may be loaded is unavailable, the DPSDBO Director is to make arrangements with the nearest DPS plant or other Navy office to utilize their microcomputer system and designate an employee to report to, and input data at that location.

The designated person will take the following items to the neighboring site:

1. The last supply "BACK-UP" disk created prior to the event which caused the system to fail.

2. All transactions that had not been entered into the system

at the time the "BACK-UP" disk was made.

3. A blank disk.

Upon arrival at the neighboring site:

1. Using the blank disk, run the supply systems' "BACK-UP" utility.

This will ensure a copy of the current data files. Label the disk to indicate it contains the neighboring sites data files.

2. Using the last "BACK-UP" disk from the inoperable microcomputer, run the supply systems' "RESTORE" utility.

At this point, the automated supply system contains all transactions that were on the "BACK-UP" disk. Enter any remaining transactions for the month and then print the end-of-month reports.

Once end-of-month reports have been printed:

1. Run the supply systems' "BACK-UP" utility using the "BACK-UP" disk to make a copy to return to present inoperable microcomputer.

2. Run the supply systems' "RESTORE" utility using the neighboring sites "BACK-UP" disk. This will return the system back to the neighboring site.

When inoperable system is again functional:

1. Run the supply systems' "RESTORE" utility, using the "BACK-UP" disk created at the neighboring site.

2. Run the "Monthly Initialization" utility and start processing for the new month.

CONTINGENCY PLAN TEST

ZENITH (PRICES APPLICATION)

SYSTEM: PRICES

TEST OBJECTIVE: To test alternate means for accomplishing normal financial transactions in case of a capture disk or hardware failure.

PERSONNEL REQUIREMENT:

NAME	TITLE	SITE

TEST SCENARIO: Hardware system breakdown which damages the DPSDBO . Option for regenerating the DPSDBO's financial capture disk would be to use another computer in the PC emulation mode.

TEST RESULTS: Using DPSDBO's hardware and financial capture disk, the project was successfully completed.

CONTINGENCY PLAN TEST

OFFICE INFORMATION SYSTEM

SYSTEM: OFFICE INFORMATION

TEST OBJECTIVE: To test alternate means for accomplishing an OIS task during an equipment failure.

PERSONNEL REQUIREMENTS:

NAME	TITLE	COMMENTS

SCENARIO: Inoperable disk drive did not allow the Director to complete a needed document. Used the another PC and completed his project using Wordstar software.

TEST RESULTS: Using the available PC, the project was successfully completed.

CONTINGENCY PLAN TEST

XEROX 6085 (ELECTRONIC PUBLISHING)

System: Xerox 6085 (Electronic Publishing)

TEST OBJECTIVE: Assuring that the use of an alternate processor will satisfy emergency requirments.

PERSONNEL REQUIREMENTS:

NAME	TITLE	COMMENTS
R. C. Blosser	Printing Officer	NPPSDBO Roosevelt Roads
E. I. Class	Secretary	NPPSDBO Roosevelt Roads
M. A. Mercado	Copy/Dup Equip Oper	NPPSDBO Roosevelt Roads

TEST SCENARIO: The file server will not power-up in to retrieve needed documents. Ms. Mercado proceeded to use the Ventura Publisher Software on the Xerox 6065 system.

TEST RESULTS: Using the alternate Desktop Publishing System the documents were produced in a timely manner.

CONTINGENCY PLAN TEST

XEROX 6065 PERSONAL COMPUTER (DESKTOP PUBLISHING)

SYSTEM: Xerox 6065 (PERSONAL COMPUTER)

TEST SCENARIO: Assuring that the use of an alternate PC will satisfy emergency requirements.

PERSONNEL REQUIREMENTS:

NAME	TITLE	COMMENTS
R. C. Blosser	Printing Officer	NPPSDBO Roosevelt Roads
E. I. Class	Secretary	NPPSDBO Roosevelt Roads
M. A. Mercado	Copy/Dup Equip Oper	NPPSDBO Roosevelt Roads

TEST SCENARIO: Inoperable disk drive in Xerox 6065 PC, disallowed the employee from completing a document. Ms. Mercado carried her disk containing the data needed to the Zenith PC and completed the document.

TEST RESULTS: Using the alternate Personal computer the mission was accomplished.

AUTOMATIC DATA PROCESSING SECURITY PLAN

Defense Printing Service
Detachment Branch Office
80 Post Lane
Camp Lejeune, N.C. 28547
13 JULY 93

TASO: SYLVIA S. KOSS
TELEPHONE: (919) 451-5919

*

Defense Printing Service
Detachment Branch Office
80 Post Lane
Camp Lejeune, N.C. 28547

1. SCOPE

The Defense Printing Service, Detachment Branch Office, Fort Bragg, (DPSDBO Fort Bragg) Automatic Data Processing Security Plan encompasses all security aspects which contribute to the protection of Automatic Data Processing (ADP) equipment and systems and Office Information Systems (OIS), both software and hardware. This applies to all ADP equipment operated in the DPSDBO Fort Bragg.

2. DIRECTOR'S POLICY STATEMENT

In accordance with OPNAVINST 5239.1 (series) the Director, Defense Printing Service Detachment Branch Office, Fort Bragg is assigned responsibility for ADP security within DPSDBO Fort Bragg, Building 8-3710. An ADP Security Plan implements those measures required to protect data against accidental or intentional disclosure to unauthorized persons and against unauthorized modification or destruction. Included within these responsibilities is the recognition of and adherence to all software copyright licensing agreements. DPSDBO Fort Bragg required copyrighted software shall not be used on personally-owned PCs or for accessing Government files from non-Government controlled work places (i.e., home, etc.). The DPSDBO Fort Bragg ADP Security Officer will take the necessary steps to provide an adequate level of security for all automatic data processing and office information equipment facilities within their area of responsibility. All personnel assigned duties of operating will utilize a risk management program which includes the following:

a. Systematically studying assets.

b. Determining the probability of loss or damage to those assets.

c. Calculating the dollar value resulting from the loss or damage to those assets.

d. Conducting a cost benefit analysis of possible countermeasures to achieve a prudent level of security.

e. Implementing those countermeasures which are cost effective.

f. Developing and implementing a local ADP Security Plan which, at a minimum, encompasses the following elements:

(1) Physical Control. To provide external protection against unauthorized access to equipment or data.

(2) Individual Accountability. Access to station identification codes, passwords, account numbers, system connect phone numbers, and data communications disks will be controlled and limited to those individuals, and data communications disks will be controlled and limited to those individuals assigned terminal access responsibilities.

(3) Data Integrity. Each file or collection of data must have an identifiable origin and use. Its use, backup, accessibility, maintenance, movement, storage, and disposition must be controlled on the basis of level and type of data, need-to-know, and other sensitive measures, as appropriate.

(4) Access Limits. Each person should have access to all of the data needed to do his/her job, but no more; i.e., an inventory manager should have access to inventory related records but not to payroll records.

(5) System Stability. An ADP system must function in a reliable and predictable manner. To minimize disruptions, power conditioning equipment will be utilized whenever practicable.

(6) Contingency Planning. Regardless of the ADP security procedures in effect, it must be assumed that an event could occur which would compromise or destroy existing data. Therefore, each ADP equipment operator must be prepared on a daily basis to prevent losing data by performing backup prior to the end of each workday. Disk with backup data will be locked in a secure and fireproof container during non-duty hours. The mandatory procedures are to be carried out and remain in effect at all times. Although ADP security is a concern of all employees, the success of the program is largely dependent on the support that management brings to it, and strict adherence by operator personnel procedures to prevent compromise or destruction of existing data.

3. ADP SECURITY ORGANIZATION AND ASSIGNED RESPONSIBILITIES

a. In accordance with OPNAVINST 5239.1 (series), an ADP Security Program is in place within DPSDBO Fort Bragg. The ADP Security Officer, DPSDBO Fort Bragg, and the ADP Security Staff (Terminal/Area Security Officers and/or Office Information System Security Officers, etc.) will take the necessary steps to provide an adequate level of security for all ADP systems and Office Information systems within the scope of the DPSDBO Fort Bragg ADP Security Program. These personnel will ensure the implementation of minimum requirements for systems developed, operated, or maintained in DPSDBO Fort Bragg.

b. The Director, DPSDBO Fort Bragg and respective ADP Security Personnel will:

(1) Develop an ADP Security Plan to provide adequate security to protect ADP systems, OI systems and automated composition systems, i.e., AGFA/Compugraphic, and the integrity of the data being handled.

(2) Be the Designated Approving Authority (DAA) for ADP/OI systems within DPSDBO Fort Bragg, as applicable.

(3) Report all ADP/OI security violations and incidents to appropriate authorities.

(4) Appoint in writing an ADPSO, TASO/ATASO, and OISSO personnel, as appropriate.

(5) Include DPSDBO Fort Bragg ADP security requirements in contracts for ADP support services.

(6) Ensure that ADP security requirements are included in life cycle management documentation as appropriate.

c. Duties and responsibilities for ADP/OI security personnel are delineated in OPNAVINST 5239.1 (series).

4. ADP SECURITY OBJECTIVES

a. To implement an ADP Security Program which is responsive to all known and recognized aspects of ADP Security.

b. To provide a practical approach to ADP security.

c. To ensure that all data handled by ADP systems and OI systems is adequately protected against inadvertent or intentional destruction, modification, disclosure, or abuse, and that users are protected against denial of service.

d. To ensure countermeasures applied for ADP security are cost effective.

e. To provide ADP/OI security awareness training to DPSDBO Fort Bragg personnel and users.

5. DPSDBO FORT BRAGG CURRENT ADP SECURITY ENVIRONMENT

a. The following narrative describes the current ADP environment within the DPSDBO Fort Bragg. The information reported herein is also found in Accreditation Schedules and ADP Security Surveys:

(1) Hardware. ADP/OI hardware currently being used by DPSDBO Fort Bragg consists of Zenith PC's, and automated phototypesetting/composition equipment.

(2) Software. Operating systems, application programs, and database management software used on site are vendor, or DPS supplied. On-the-shelf programs (LOTUS, dBASE, Multimate, etc.) are also used for various operational applications.

(3) Physical Facility/Security. The DPSDBO Fort Bragg Security Officer/ADP Security Officer is responsible for overall physical security and the implementation and operation of all ADP security controls. The Director is responsible for his/her physical facility/internal security programs in compliance with OPNAVINSTs 5510.1 and 5530.14 (series).

(4) Personnel Security. All ADP employees, terminal operators, and other personnel required to have regular access to DPSDBO Fort Bragg ADP systems are issued access in accordance with OPNAVINST 5239.1 (series), NAVPUBINST 5239.1 (series), and NPPS SOEASTAREAINST 5239.1 (series). The

Director, DPSDBO Fort Bragg, is responsible for compliance with current directives.

(5) Emanations. No classified or sensitive data is processed with DPSDBO Fort Bragg, according to current regulations and directives.

(6) Administrative/Operating Procedures. NAVPUBINST 5239.1 and NPPS SOEASTAREAINST 5239.1 (series) are the current guidelines for ADP security requirements. These instructions comply with the requirements of OPNAVINST 5239.1 (series).

(7) Data. Only a very minimal amount of Level II data is processed. Overall levels of data being processed on DPSDBO Fort Bragg ADP systems are as follows:

(a) Level I - 0%
(b) Level II - 80%
(c) Level III - 20%

(8) Training. Training is provided for ADPSO, TASO'S, and OISSO's in accordance with OPNAV, NAVPUB, and NPPS SOEASTAREA Instructions in the 5239.1 (series). On-the-job security training for terminal operators is provided as required.

(9) Audit/Internal Review. Security reviews of ADP systems are performed, and internal audits of DPS facilities are performed by higher echelon commands.

(10) Life Cycle Management. Life cycle management guidelines are currently being applied in system development efforts within DPS, SOEASTAREA.

6. PLAN INTRODUCTION

a. INTRODUCTION

(1) PURPOPSE. To establish and implement the Contingency Plan for Defense Printing Service Detachment Branch Fort Bragg, ADP/OIS systems. This plan provided essential guidance for contingency preparations, emergency reactions, and back-up operations following the occurrence of contingency situations.

(2) OBJECTIVES

(a) Adverse incidents are normally followed by periods of disorientation. The failure to react to contingency situations in a preconceived manner often results in losses greater than those caused by the incident.

(b) Losses following contingency occurrences can be reduced by assessing the operational environment, planning courses of action, assigning responsibilities for those actions, and ensuring that the actions will occur through practice. The accomplishment of these attributes is the central objective of this plan.

b. PLANNING CONSIDERATIONS

(1) MISSION. The primary mission of DPSDBO Fort Bragg is to provide printing and publications services to Department of Defense and Federal agencies within the area. Operational (production) responsibility for printing services is under the authority of the Joint Committee on Printing, Congress of the United States (JCP).

(2) EXISTING PROGRAMMED CAPABILITIES. DPSDBO Fort Bragg currently operates an automated printing management system. Other automated systems currently operational include automated composition and editing, and systems operated in support of Defense Printing Service's reprographic equipment and printing production efforts. OIS systems which handle the processing of Level II and Level III data are also operational within DPSDBO Fort Bragg.

(3) ENVIRONMENTAL ASSESSMENT. In determining the scope of this contingency plan, risk assessments of the DPSDBO Fort Bragg systems were used to evaluate the operational environment and resultant contingency requirements.

(4) RISK ASSESSMENT. The risk assessments were completed in conjunction with the development of this plan. Through this process, potential threats and their impact on DPSDBO Fort Bragg sources were identified and evaluated. Cost-effective countermeasures have since been identified and are being implemented to minimize possible losses from these threats.

(5) WORKLOAD EVALUATION AND PRIORITIZATION

(a) A primary concern in developing this plan was to carefully arrive at an economic balance between adequate protection and the cost of that protection.

(b) Consideration was given to the fact that DPSDBO Fort Bragg currently maintains other systems that are self-standing, special purpose units utilized in support of the printing and publications process which involve no transmission of data nor interaction with a host mainframe. OI systems overall do not utilize any transmission of data, and no OI system within DPSDBO Fort Bragg is authorized to handle Level I data.

(6) CRITICAL DEPENDENCIES

(a) DPSDBO Fort Bragg contingency for continuous operations data capture and transmission is facilitated by the use of like equipment and operational instructions at all DPS locations. In the majority of cases, if an emergency incapacitates one facility, the responsibility for the ADP support of that facility is then transferred to the next nearest DPS location.

(b) If mutual support agreements are necessary, they will be established with other DPS automated activities. These agreements commit the processing resources of supporting activities, often referred to as "back-up-sites", to the local contingency reaction effort.

(c) Potential emergencies anticipated to have a high probability which would cause a disruption of service include hardware failure, data capture disk failure, and operator error. While any reasonable disruption of service would be an annoyance, it would not have a serious impact on the DPSDBO Fort Bragg mission.

c. PLANNING ASSUMPTIONS. This plan is based upon the current workload, procedures, and capabilities of DPSDBO Fort Bragg. To establish and maintain a planning base, the following assumptions were drawn and used in the development of this plan:

(1) The current risk assessments considered all of the potential threats that should be accounted for, reflect accurately calculated annual loss expectancies (ALES), and properly indicate residual risk.

(2) Subsequent risk assessments will be conducted at the frequency required by the DPS ADP Security Program.

(3) This plan will be validated against the results of future risk assessments to ensure its continuinmg currency.

(4) The procedures provided in this plan will be kept current with the capabilities of DPSDBO Fort Bragg systems.

(5) Where necessary, back-up copies of system software, applications systems, program files, and all supporting documentation are maintained on-site in a manner that will allow necessary retrieval of same.

(6) This plan will be tested annually as required by Department of the Navy ADP Security policy.

d. STRUCTURE OF THE PLAN

(1) Part 1 of the plan contains those prepatory actions necessary to ensure rapid implementation of the remainder of the plan. Items detailed in this section include requirements to establish and maintain application backups and the training of all system personnel.

(2) Part II of the plan specifies actions to be taken to ensure continuity of operations following a reduction or loss of local processing capability and contains the procedures to follow when a component's capability has been reduced or a system is unavailable for extended periods of time. Included is an identification of alternative processing sites.

7. PART 1 - CONTINGENCY PREPARATION. During the planning process, it was determined that the readiness of DPS, SOEASTAREA facilities to respond to an ADP/OI contingency situation is dependent upon the currency of such essential information as the requirements for a back-up processing capability, personnel training, and the identification of which personnel are to be trained in contingency situations.

a. APPLICATION BACKUP

(1) The ability to continue operations after a contingency situation occurs is largely dependent upon ensuring that applications

software survives the emergency. For this reason, a primary thrust of contingency preparation is to ensure the survival of important software. For each application, the need to back up individual programs, data and documentation depends in part on how these items were obtained originally.

(2) In determining the software back-up requirements for DPS, SOEASTAREA systems, it was obvious that all locally produced software must be backed up locally. Software obtained from outside sources need only be backed up locally if additional copies cannot be obtained from outside sources within a reasonable time. Back-up requirements have been identified for applications processed by DPS SOEASTAREA systems and have been incorporated into the daily procedures as follows:

(a) Backups of any programs will be made after any new receipt/change.

(b) Backups of data will be made following each update of a data file, or at the end of each work day.

(3) Additionally, two copies of program software and data files which are not retrieveable through DPSMO, Washington, vendor support, or other DPS SOEASTAREA components, are produced to support this plan. One copy is used as a working copy to accomplish normal processing. A second "on-site" back-up copy is stored in a fireproof container away from the processing site. The original program software, where possible and feasible, will be stored at an off-site location.

b. CONTINGENCY REACTION PERSONNEL. From an economic view, it is unrealistic to expect to be able to train all personnel to respond appropriately when processing contingencies arise. At the same time, key DPSDBO Fort Bragg personnel must be ready to respond to these situations with minimal delay and acceptable proficiency. The DPSDBO Fort Bragg TASO will be cognizant of all contingency requirements.

c. CONTINGENCY PLAN TESTING. This plan will be tested initially and at least annually thereafter. Future tests will simulate operational scenarios and will be conducted and documented as required.

8. PART II - CONTINGENCY REACTION PLAN

a. PROCEDURES GOVERNING DPS SOEASTAREA SYSTEMS

(1) In the event that the automated data processing capability at DPSDBO Fort Bragg is incapacitated for a period in excess of ten working days, it will be brought to the attention of the DPS, SOEASTAREA ADP Security Officer (ADPSO)/Security Manager.

(2) The ADPSO will coordinate equipment and personnel logistics as required and maintain a log of equipment relocations.

b. FINANCIAL SYSTEM

(1) DPS automatic data processing support for the Financial System is furnished by NARDAC via an interagency agreement. The NARDAC acts an ADP Service Center for DPS and other users of their systems. They provide,

on a reimbursable basis for telecommunications services, the housing of applications and system software, transmitted data, and for processing DPS data.

(2) NARDAC provides the provision of alternate site processing of its users' applications in emergency situations. NARDAC has a similar configuration of ADP support equipment and is capable of supporting DPS should an emergency arise. DPS data files are stored off-site from the data processing center, and provisions are incorporated in the DPS interagency agreement for contingency emergency support.

c. SUPPLY SYSTEM

(1) DPSDBO Fort Bragg ADP program support for the Supply System is furnished by DPSDO Charleston. In the event that the DPSDO Charleston computer system is inoperative and would remain so for a period of time that would affect the end-of-month reporting, the following back-up/recovery operations will apply. If a second microcomputer where the supply system may be loaded is unavailable, the DPSDBO Fort Bragg Director will make arrangements with the nearest DPS plant or other Army or Navy office to utilize their microcomputer system and designate an employee to report to and input data at that location. The designated person will take the following items to the neighboring site:

- The last Supply "BACK-UP" disk created prior to the event which caused the system to fail.

- All transactions that had not been entered into the system at the time the "BACK-UP" disk was made.

- A blank disk.

(2) Using the blank disk, run the Supply System's "BACK-UP" utility. Note: This will ensure a copy of the current data files. Label the disk to indicate it contains the neighboring sites' data files.

(3) Usisng the last "BACK-UP" disk from the inoperable microcomputer, run the Supply System's "RESTORE" utility.

- At this point, the automated supply system contains all transactions that were on the "BACK-UP" disk. Enter any remaining transactions for the month and then print the end-of-month reports.

(4) Once end-of-month reports have been printed:

- Run the Supply System's "BACK-UP" utility using the "BACK-UP" disk to make a copy to return to present inoperable microcomputer.

- Run the Supply System's "RESTORE" utility using the neighboring site's "BAKC-UP" disk. This will return the system back to the neighboring site.

(5) When inoperable system is again functional:

- Run the Supply System's "RESTORE" utility, using the "BACK-UP" disk created at the neighboring site.

- Run the "Monthly Initialization" utility and start processing for the new month.

d. ALTERNATE PROCESSING SITES. Data capture and transmission capability within the DPS, SOEASTAREA are located at DPS, SOEASTAREA Headquarters; DPSDO, Charleston; DPSDO, Norfolk; and DPSDO, Fort Eustis. Electronic page printing systems in DPS, SOEASTAREA are currently located at DPSDO, Charleston; DPSDO, Norfolk; DPSDO, Fort Eustis; and DPSDBO, Portsmouth. These sites will serve as alternate ADP support sites for each other. For microcomputer based applications, the nearest available microcomputer will be used.

TERMINAL SECURITY INSPECTION CHECKLIST

ACTIVITY Defense Printing Service Branch Office, Camp Lejeune, N.C. 28542-50

TASO Sylvia S. Koss DATE 6-26-92

PHONE (919) 451-5919/5131 AUTOVON 484-5919/5131

		YES	NO	N/A	COMMENTS
1.	Has an ADP Terminal Area Security Officer (TASO) been appointed in writing? NAME Sylvia S. Koss OFFICE CODE 48994 PHONE (919) 451-5919/5131 AV 484-5919/5131	X			
2.	List the Terminal ID numbers used at this physical location. SYSTEM 01	X			
3.	Is the Terminal Area designated as a controlled area and have the proper signs been posted? (i.e. "RESTRICTED AREA" or "AUTHORIZED PERSONNEL ONLY")	X			
4.	Is a current Terminal Area Access Roster posted in the terminal area to identify authorized users?	X			
5.	Do all users having access to the terminal have a <u>need</u> to use the terminal?	X			

		YES	NO	N/A	COMMENTS
6.	Are all projected changes to the Access Roster (additions/deletions) identified in a timely manner?	X			
7.	Have written Terminal Area procedures been supplied to identify TASO and user responsibilities?	X			
8.	Are devices containing oscillators, such as radios, televisions, tape players, etc. located within 10 feet of any terminal?		X		
9.	Is the terminal area secured				
	During Duty Hours?	X			
	After Duty Hours?	X			
10.	Is the Terminal Area free of accumulated trash?	X			
11.	Are only terminal operators who have passwords allowed to use terminals?	X			
12.	Does the TASO maintain a file of security directives?	X			
13.	Are terminals monitored for proper use?	X			
14.	Are ADP media and printouts containing Personal Data (Privacy Act Data) and Business sensitive data properly labeled?	X			
15.	Are training records on file showing that each user is briefed quarterly on Terminal security requirements and emergency procedures?	X			

	YES	NO	N/A	COMMENTS
16. Are security problems reported to the ADP Security Officer?	X			
17. Is the destruction of waste output in accordance with OPNAVINST 5510.1 (series)?	X			
18. Are passwords and dial-up telephone numbers protected by locking in a secure container, where appropriate?	X			
19. Are system Terminal(s) inactivated and protected when unauthorized personnel are present?	X			

TERMINAL SECURITY INSPECTION CHECKLIST

ACTIVITY Defense Printing Service Branch Office, Camp Lejeune, N.C. 28542-50

TASO Svlvia S. Koss

DATE 6-26-92

PHONE (919) 451-5919/5131

AUTOVON 484-5919/5131

		YES	NO	N/A	COMMENTS
1.	Has an ADP Terminal Area Security Officer (TASO) been appointed in writing? NAME Sylvia S. Koss OFFICE CODE 48994 PHONE (919) 451-5919/5131 AV 484-5919/5131	X			
2.	List the Terminal ID numbers used at this physical location. SYSTEM 02	X			
3.	Is the Terminal Area designated as a controlled area and have the proper signs been posted? (i.e. "RESTRICTED AREA" or "AUTHORIZED PERSONNEL ONLY")	X			
4.	Is a current Terminal Area Access Roster posted in the terminal area to identify authorized users?	X			
5.	Do all users having access to the terminal have a <u>need</u> to use the terminal?	X			

	YES	NO	N/A	COMMENTS
6. Are all projected changes to the Access Roster (additions/deletions) identified in a timely manner?	X			
7. Have written Terminal Area procedures been supplied to identify TASO and user responsibilities?	X			
8. Are devices containing oscillators, such as radios, televisions, tape players, etc. located within 10 feet of any terminal?		X		
9. Is the terminal area secured				
During Duty Hours?	X			
After Duty Hours?	X			
10. Is the Terminal Area free of accumulated trash?	X			
11. Are only terminal operators who have passwords allowed to use terminals?	X			
12. Does the TASO maintain a file of security directives?	X			
13. Are terminals monitored for proper use?	X			
14. Are ADP media and printouts containing Personal Data (Privacy Act Data) and Business sensitive data properly labeled?	X			
15. Are training records on file showing that each user is briefed quarterly on Terminal security requirements and emergency procedures?	X			

	YES	NO	N/A	COMMENTS
16. Are security problems reported to the ADP Security Officer?	X			
17. Is the destruction of waste output in accordance with OPNAVINST 5510.1 (series)?	X			
18. Are passwords and dial-up telephone numbers protected by locking in a secure container, where appropriate?	X			
19. Are system Terminal(s) inactivated and protected when unauthorized personnel are present?	X			

ASSET VALUATION WORKSHEET

1. ASSET NAME

Pesmis

2. ASSET DESCRIPTION AND JUSTIFICATION OF IMPACT VALUE RATINGS ASSIGNED.

Hardware

One Z-248 microcomputer with 20 mB hard Disk Drive + one Floppy disk Drive w/ Color monitor.	$2,400.00
MPI-180 FT printer -	1,230.00
AB Switch Data transfer -	14.00
Surge protection Strip -	4.95
Hayes Modem 9600	399.00
total asset Value:	4,047.95

Data

Utilizing the Impact Category of the Disclosure resulted in the highest impact Value. Disclosure of Level II data was assigned a Value of $3,000.00 (table E-2 of Opnav 5239.1A)

Software

Utilizing the Impact Category of Destruction resulted in the highest impact Value, the Value of the hardware assets consists of the total replacement

3. IMPACT VALUE RATING BY IMPACT AREA

☐ MODIFICATION ☐ DESTRUCTION ☐ DISCLOSURE ☐ DENIAL OF SERVICE

ASSET VALUATION WORKSHEET

1. ASSET NAME

Primis

2. ASSET DESCRIPTION AND JUSTIFICATION OF IMPACT VALUE RATINGS ASSIGNED.

Costs of the Operating & Application Software and the time required to restore Systems.

Cost to replace comercial Software is $80.00.

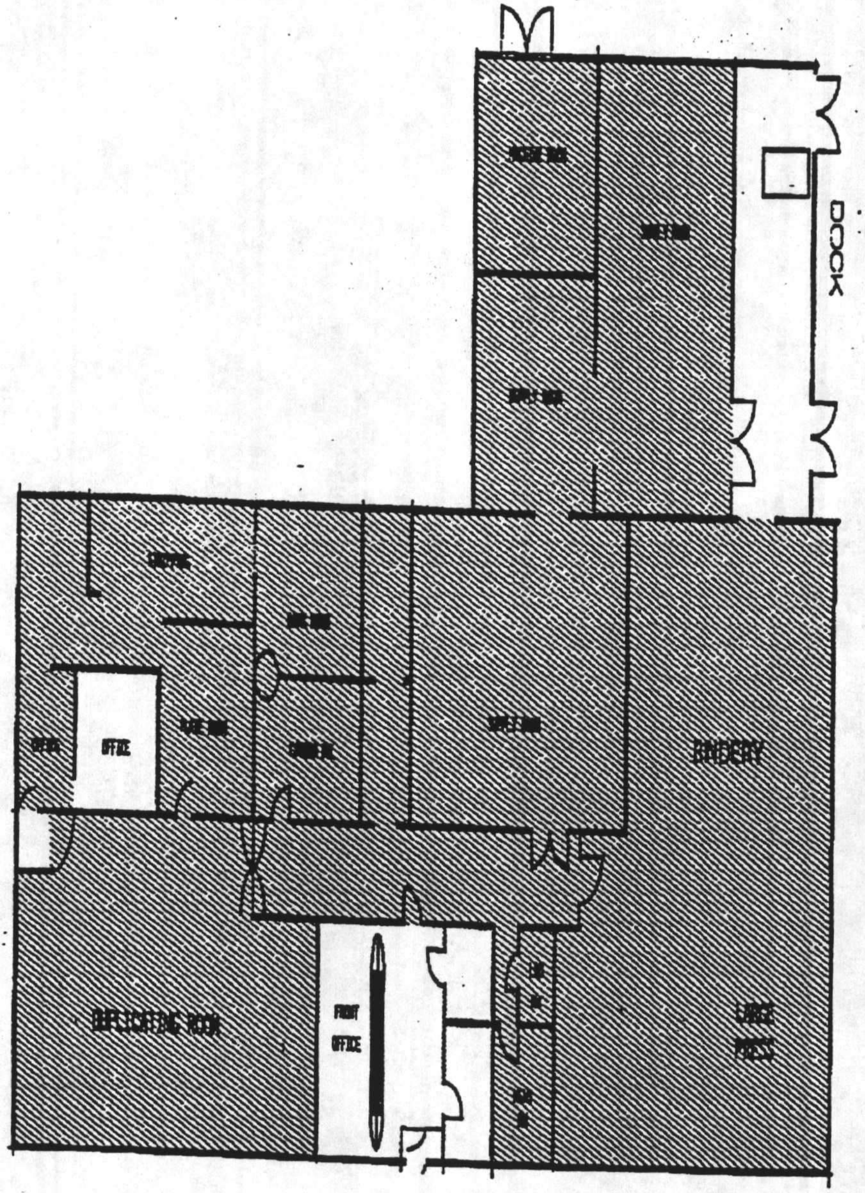
Six hours estimated for a GS-4, Data transcriber to restore Systems is (15,171 divided by 2087 X 1.38)

$60.11

3. IMPACT VALUE RATING BY IMPACT AREA

□ MODIFICATION □ DESTRUCTION □ DISCLOSURE □ DENIAL OF SERVICE

DPSDBO CAMP LEJEUNE



▨ RESTRICTED AREA

ATTACHMENT V-E

(PAGE 1)

ACTIVITY ACCREDITATION SCHEDULE

NPRS-SOEASTDIV-5239/1 (5-83)

UNIT IDENTIFICATION CODE *(UIC)*
48994

ACTIVITY NAME AND ADDRESS
Director
Defense Printing Service
Detachment Branch Office
80 Post Lane
Camp Lejeune, N.C. 28547

DIRECTOR'S NAME
L. C. Bradley

AUTOVON TELEPHONE NO.
484-5919

COMMERCIAL TELEPHONE NO.
(919) 451-5919

TA SECURITY OFFICER'S NAME
Sylvia S. Koss

AUTOVON TELEPHONE NO.
484-5919

COMMERCIAL TELEPHONE NO.
(919) 451-5919

DAA				LEVEL OF PROCESSED DATA			MODES OF OPERATION				ACTIVITY ADP ELEMENTS					
SOEASTDIV	NPPSMO/ COMNAVDAC	DIR. NIS	CNO	I	II	III	LIMITED	DEDICATED	CONTROLLED	MULTILEVEL	APPLICATION NAME	HARDWARE (CPU) MFG	SOFTWARE (OPER. SYS.)	FACILITY BLDG NO. ROOM NO.	COMMUNICATIONS: NUMBER OF NODES (LOCATIONS) AND TERMINALS	NETWORKS NAMES (S)
X					X	X	X				PRMIS SN627AH0123	ZENITH Z-248	COST AND FINANCIAL	BLDG. 80	1	Z-CAPS
X					X	X	X				Z-CAPS AUTO-MATED PRICING SN842AF00600	ZENITH Z-248	MS-DOS	BLDG. 80	1	Z-CAPS/LAN
X					X	X	X				SN627AH0123	ZENITH Z-248	PRICES	BLDG. 80	1	N/A

(Page 2)

ACTIVITY ACCREDITATION SCHEDULE

NPPS-SOEASTDIV-5239/1 (5-83)(Back)

ACTIVITY ADP ELEMENTS *(Continued)*							ESTIMATED SCHEDULE				NAME OF TERMINAL AREA SECURITY OFFICER (TASO)
TEMPEST REQUIRED *(If yes provide task number)*			COMSEC REQUIRED		DES REQUIRED		RISK ASSESSMENT: ESTIMATED START/ COMPLETION DATES	ST & E: PLAN DEVELOPMENT DATE, TEST DATE	CONTINGENCY PLAN DEVELOPMENT DATE	REQUEST FOR ACCREDITATION SUBMISSION DATE	
NO	YES	TASK NUMBER	NO	YES	NO	YES					
X			X		X		May 93	June 93	June 93	June 93	SYLVIA S. KOSS
X			X		X		May 93	June 93	June 93	June 93	SYLVIA S. KOSS
X			X		X		May 93	June 93	June 93	June 93	SYLVIA S. KOSS