



COMDTINST M5500.17  
16 AUG 1989

COMMANDANT INSTRUCTION M5500.17

Subj: Standard Workstation Security Handbook

Ref: (a) COMDTINST M5500.13(Series), Automated Information  
System (AIS) Security Manual

1. PURPOSE. This manual provides Coast Guard policy, procedures, standards, and guidance for implementing the Automated Information Systems (AIS) Security Program on the Standard Workstation.
2. BACKGROUND. Reference (a) provides overall AIS security policy, procedures, standards, and reporting requirements. The AIS Security Manual, though inclusive, did not provide a low level of detail for the typical Coast Guard Standard Workstation. An easy to read, quick reference handbook was needed to effect implementation of the AIS Security Program's policies and procedures for the Standard Workstation.
3. DISCUSSION. This handbook is a single reference for USCG Standard Workstation AIS Security policy and procedures. It refers to and amplifies policy contained in reference (a).
4. ACTION. Area and district commanders, commanders of maintenance and logistics commands, unit commanding officers, Commander, CG Activities Europe, chiefs of offices and special staff divisions at Headquarters shall ensure implementation and compliance with this manual.

/s/ R. M. POLANT  
Chief, Office of Command,  
Control & Communications

TABLE OF CONTENTS

	<u>PAGE</u>
CHAPTER 1. STANDARD WORKSTATION SECURITY OVERVIEW AND POLICY	
A. PURPOSE.....	1-1
B. SCOPE AND APPLICABILITY.....	1-1
C. DEFINITIONS.....	1-1
D. POLICY.....	1-3
E. HIERARCHY.....	1-3
F. PRECEDENTS.....	1-4
CHAPTER 2. STANDARD WORKSTATION SECURITY IMPLEMENTATION	
A. ACCREDITATION.....	2-1
B. ACCREDITATION AUTHORITY.....	2-3
C. STANDARD WORKSTATION ACCREDITATION REQUIREMENTS....	2-3
1. ADP Systems Security Officer (ADPSSO).....	2-3
2. System Classification/Sensitivity Level.....	2-3
3. AIS Security Plan.....	2-4
4. Risk Assessment.....	2-4
5. Contingency Plan.....	2-5
6. Security Test and Evaluation.....	2-5
7. Accreditation Letter/Memo.....	2-6
8. Re-accreditation.....	2-6
9. Interim Authority to Operate.....	2-6
D. OTHER STANDARD WORKSTATION SECURITY REQUIREMENTS...	2-7
1. Classified Processing.....	2-7
2. Personnel Security.....	2-7
3. Security Awareness and Training.....	2-8
4. Self-Audit Report.....	2-8
5. Sensitive Application Certification.....	2-8
CHAPTER 3. SECURITY CONTROLS	
A. GENERAL.....	3-1
B. PHYSICAL CONTROLS.....	3-1
C. ADMINISTRATIVE CONTROLS.....	3-1
1. System Usage.....	3-1
2. Backup.....	3-1
3. Backup Storage.....	3-1
4. Passwords.....	3-2
5. Application/Utility Access.....	3-3
6. Volume/Directory/File Protection.....	3-3
7. Software Licenses.....	3-4
8. Public Domain Software.....	3-4
9. Individual Use of Standard Workstations.....	3-4
10. Miscellaneous.....	3-5

TABLE OF CONTENTS

	<u>PAGE</u>
FIGURES	
FIGURE 1-1. AIS SECURITY HIERARCHY.....	1-5
FIGURE 2-2. ACCREDITATION PROCESS.....	2-2
ENCLOSURES	
ENCLOSURE (1) - Sample AIS Security Plan	
ENCLOSURE (2) - Sample Contingency Plan Set	
ENCLOSURE (3) - Sample Letter/Memo of Accreditation	
ENCLOSURE (4) - Examples of Customized User Command Sets	

CHAPTER 1. STANDARD WORKSTATION SECURITY OVERVIEW AND POLICY

- A. PURPOSE. This Handbook presents strategies and procedures for implementing the policies, requirements, and standards of COMDTINST M5500.13 series, Automated Information Systems (AIS) Security Manual.
- B. SCOPE AND APPLICABILITY. The AIS Security Manual provides overall AIS security policy, principles, standards, management procedures, and reporting requirements. The AIS Security Manual is the foundation of the AIS Security program which implements Department of Transportation policy, Office of Management and Budget (OMB) Circular A-130, and the Computer Security Act of 1987 (P.L. 100-235). This Handbook is a single reference for implementation of AIS security policy and procedures for the USCG Standard Workstation. It refers to and amplifies Commandant policy as contained in the AIS Security Manual. This Handbook applies to all Standard Workstation systems owned by or operated on behalf of the Coast Guard.
- C. DEFINITIONS. Definitions applicable to computer security and automated information systems are contained in Chapter 1 and Enclosure (1) of COMDTINST M5500.13 series, AIS Security Manual. A limited set of security definitions are provided here.
1. Accreditation. The official authorization granted to a Standard Workstation system to process classified or sensitive information in its operational environment. Accreditation is based on the determination that the Standard Workstation system is operating at an acceptable level of risk, after a security evaluation and consideration of other management factors (e.g., criticalness of operations, cost to implement controls, impact on operations, etc.)
  2. Certification. The official authorization that is granted to a sensitive application attesting to the adequacy of its security controls. Certification is made based on an independent review of security controls of an application and the manual interfaces with that application. The review determines if security design specifications for the application are correct and have been properly implemented. The USCG has issued guidance for sensitive applications in the Sensitive Application Design Guide (SADG) and the Sensitive Application Certification Review Methodology (see enclosures to the AIS Security Manual)
  3. Contingency Plan. A contingency plan provides a course of action to be followed during or following an emergency or other abnormal event which causes or may cause a disruption in processing services for essential functions (applications). Contingency plans address both the data processing support and the function itself. There are four parts to a contingency plan: emergency response (immediate action to an event); backup operations (temporary restoration of operations); disaster assessment (a judgment on the severity of the event); and recovery actions (actions required for permanent restoration of operations).

- 1.C.4. Data/System Sensitivity Levels (I, II, III). Categories used to determine the degree of protection to be afforded data or Standard Workstation systems used to process that data. ALL USCG Standard Workstation systems shall be designated Level I or Level II. No Standard Workstation system shall be designated Level III.
- a. Classified (Level I) is classified data or a system used to process classified data.
  - b. Sensitive (Level II) is sensitive data or systems used to process sensitive data. See Sensitive Information (Data), paragraph C.8.
  - c. Non-sensitive (Level III) is Information which does not warrant a higher designation.
5. Designated Approving Authority (DAA). The DAA is the official responsible for accrediting a Standard Workstation system and certifying sensitive application systems. In this case the DAAs are; area and district commanders, commanders of maintenance and logistics commands, Headquarters unit commanding officers, Commander CG Activities Europe, and chiefs of offices at Headquarters. This official assumes the responsibility that all requirements for accreditation have been met and that the system is operating within an acceptable level of risk. Commanding Officers of local activities have the authority to issue an interim authority to operate. See chapter 2, paragraph B.
6. Risk Assessment (or Risk Analysis). This is an analysis of assets and vulnerabilities, and threats to those assets to determine the level of risk to a Standard Workstation system. Various methodologies exist which either quantify or qualify the risk. The USCG has developed a methodology specifically for the Standard Workstation, the Standard Terminal Risk Assessment Methodology (STRAM). This methodology shall be used for performing risk assessments of Standard Workstation systems.
7. Sensitive Application. An application is considered sensitive if it contains or processes classified information, sensitive information (e.g. financial/accounting information, personnel data) or is an integral part of operations such that its loss or subversion could result in failure of the activity to complete its mission (i.e. mission critical). See paragraph C.8.

1.C.8. Sensitive Information (or Data). The term "sensitive information" means, any information that; the loss or misuse of, unauthorized access to, or modification of, could adversely affect the national interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the privacy act). This is information that has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. Examples of sensitive information include personal, budget, financial and management information, and information generally categorized as For Official Use Only (e.g., proprietary and privileged information). Classified information is a separate category of information, and is always designated as classified (e.g., Confidential, Secret, Top Secret).

D. POLICY. All Coast Guard personnel shall:

1. Protect AIS Resources. Provide adequate and effective protection of all AIS resources, including computer facilities and equipment, peripheral, remote terminals, programs, associated documentation, supplies, information, and personnel associated with computer operations.
2. Protect Classified and Sensitive Information. Protect classified and sensitive information handled by automated systems against espionage, sabotage, fraud, misappropriation, misuse, or compromise. The information categories include classified, unclassified national security-related, Privacy Act, privileged, proprietary, and that designated "For Official Use Only"; and other information which must be protected from unauthorized disclosure, alteration, loss, or destruction because of possible damage to personnel or property.
3. Protect Funds, Supplies, and Materiel. Protect funds, supplies, and materiel managed or disbursed through the use of a Standard Workstation from theft, fraud, misappropriation, or misuse. This includes Standard Workstations which are involved in the control and distribution of funds (e.g. PMIS/JUMP, ARMS, LUFs, SUFS), or the processing of information which offers the opportunity to divert economically valuable resources (e.g., supplies, dollars, or information).

E. HIERARCHY. To put execution of the security requirements in perspective, an understanding of the AIS security program hierarchy is needed.

1. Overall Coast Guard Security. Commandant (G-O) is the program director for Coast Guard security overall and the Chief, Intelligence, Investigations and Security Division (G-OIS) is the program manager.
2. AIS Security. Commandant (G-T) is the program director for AIS security and Commandant (G-TIS) is the program manager.

- 1.E.3. Communication Security. Commandant (G-T) is the program director for Communication security (COMSEC/TEMPEST) and Commandant (G-TTS) is the program manager.
4. AIS Security Implementation. Area and district commanders, commanders of maintenance and logistics commands, Headquarters unit commanding officers, Commander CG Activities Europe, and chiefs of offices at Headquarters implement AIS security policy, principles, and standards, contained in the AIS Security Manual and this manual within their command or office.
5. ADP Security Officer (ADPSO). An ADP Security Officer (ADPSO) shall be appointed by those listed in paragraph E.4. above. The ADPSO is the focal point for the AIS Security Program within the command's organization (e.g., within a Headquarters office or district). The ADPSO is responsible for all subordinate units to the command.
6. ADP System Security Officer (ADPSSO). An ADP System Security Officer (ADPSSO) shall be appointed for each Standard Workstation cluster or stand-alone system. One ADPSSO may be responsible for several Standard Workstation systems. The ADPSSO may be any Coast Guard employee (civilian or military) with an appropriate clearance or background investigation for the sensitivity level of the system. The ADPSSO should have sufficient knowledge of the system to implement AIS security. At smaller Headquarters offices or Headquarters unit the ADPSO may also be an ADPSSO.
7. AIS Security Hierarchy Schematic. See figure 1-1 for a schematic of the hierarchy. A complete discussion of responsibilities is contained in Chapter 2, "Areas of Responsibility," of the AIS Security Manual.
- F. PRECEDENTS. The AIS Security Program is a sub-program of the Coast Guard Security Program. In the event of conflict between the requirements of this Handbook, the AIS Security Manual and COMDTINST M5500.11 series, Security Manual, the requirements of COMDTINST M5500.11 series take precedent. Conflicts in requirements may also occur when other department/agency security requirements are applicable. If an official with command responsibility determines that a conflict in requirements exists, he shall notify Commandant (G-OIS) and Commandant (G-TIS) of the conflict in writing.

AIS SECURITY HIERARCHY

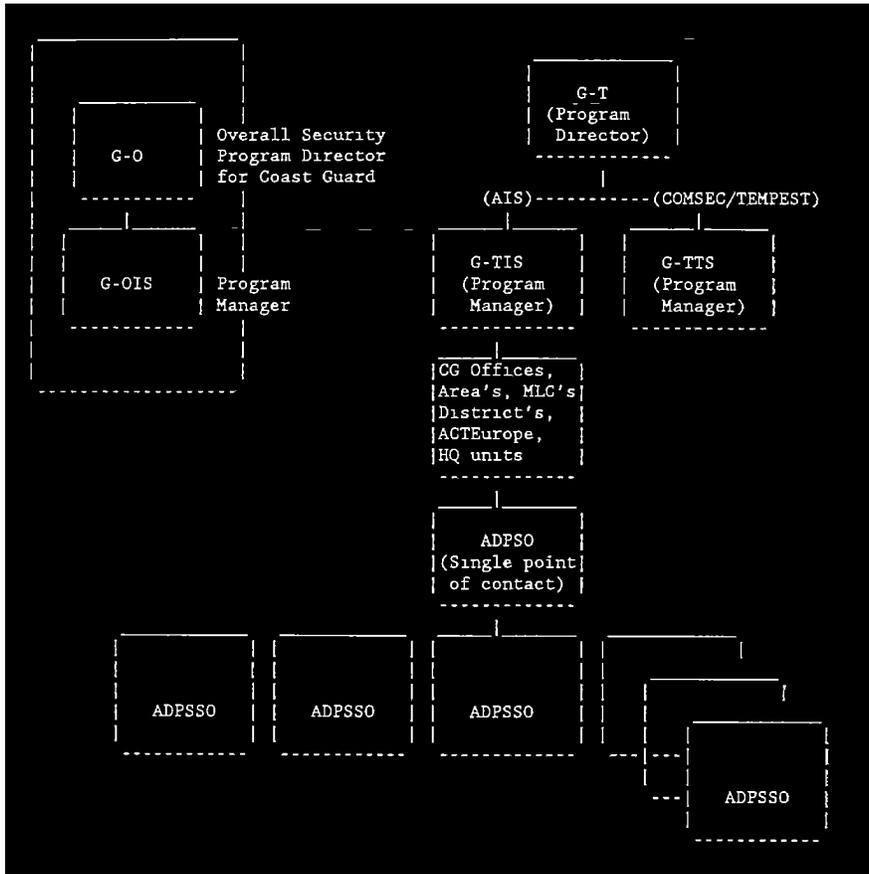


Figure 1-1

## CHAPTER 2. STANDARD WORKSTATION SECURITY IMPLEMENTATION

- A. ACCREDITATION. An activity's security program must identify, reduce, and control risk. This is accomplished through system accreditation and re-accreditation. Accreditation is the formal declaration that appropriate security controls have been implemented for a Standard Workstation system (cluster or stand-alone). The requirement for accreditation applies to all Coast Guard Standard Workstation systems. For a Standard Workstation system to be accredited the following requirements must be satisfied:
1. ADPSSO. An ADPSSO shall be appointed in writing for each Standard Workstation system. See paragraph C.1 .
  2. AIS Security Plan. An AIS Security Plan shall be written and updated annually. See paragraph C.3.
  3. Risk Assessment. A risk assessment shall be conducted for each Standard Workstation system. See paragraph C.4.
  4. Contingency Plan. A contingency plan shall be prepared for each Standard Workstation system and updated annually. See paragraph C.5.
  5. Letter/Memo of Accreditation. An Accreditation Letter/Memo shall be sent to the Designated Approving Authority (DAA) for signature. Supporting documentation must accompany the letter. See paragraph C.7.
  6. DAA Signature. The DAA shall review the accreditation support documentation identified above (paragraphs A.1 through A.5) and either concur, thereby declaring that a satisfactory level of AIS security is present; or not concur, indicating that the level of risk either has not been adequately defined or has not been reduced to an acceptable level for Standard Workstation operations. A Standard Workstation system may be granted an interim authority to operate, in accordance with paragraph C.8. of this chapter.
  7. Accreditation Process Schematic. See figure 2-1 for a schematic of the accreditation process. A requirement which is not part of the accreditation process is the certification of sensitive applications. This process is described in Chapter 14, "Sensitive Application Certification," of the AIS Security Manual.

ACCREDITATION PROCESS

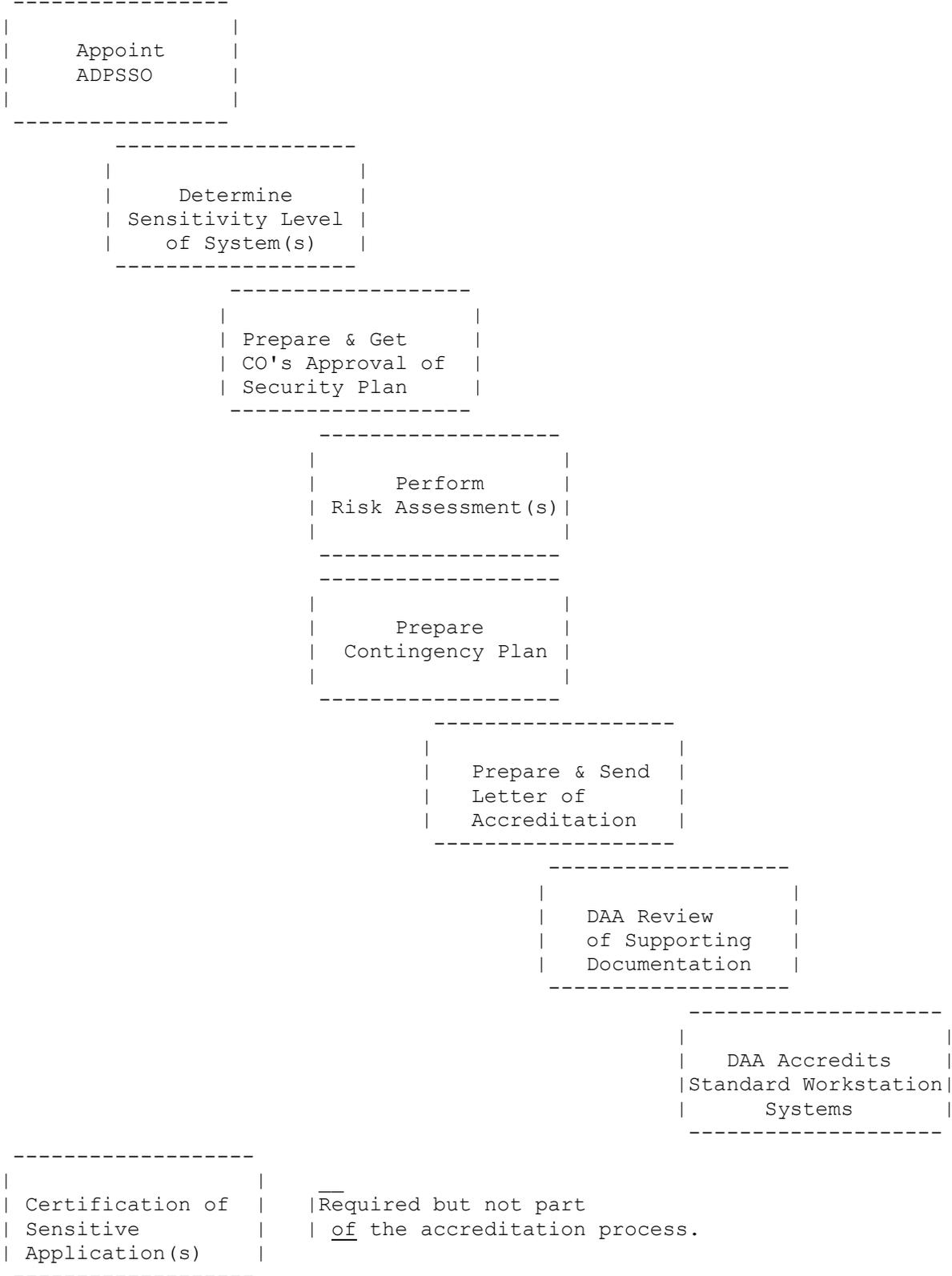


Figure 2-1  
2-2

2.B. ACCREDITATION AUTHORITY. The classification/sensitivity of the data processed by a Standard Workstation system determines who is the DAA for that system. The appropriate DAA is indicated below:

1. Classified Standard Workstation Clusters. Clustered systems processing or storing classified data shall be accredited by Commandant (G-T).
2. Classified Stand-alone Standard Workstations. Stand-alone systems processing or storing classified data shall be accredited by; area and district commanders, commanders of maintenance and logistics commands, Headquarters unit commanding officers, Commander CG Activities Europe, and chiefs of offices at Headquarters. In addition to satisfying the accreditation requirements, these system must be operated in accordance with the requirements of Chapter 18, "Classified Information Processing," of the AIS Security Manual.
3. Unclassified Standard Workstation Ssystems. All unclassified Standard Workstation systems shall be accredited by area and district commanders, commanders of maintenance and logistics commands, Headquarters unit commanding officers, Commander CG Activities Europe, and chiefs of offices at Headquarters.

C. STANDARD WORKSTATION ACCREDITATION REQUIREMENTS.

1. ADP Systems Security Officer (ADPSSO). Area and district commanders, commanders of maintenance and logistics commands, unit commanding officers/officers in charge, Commander CG Activities Europe, chief of offices and special staff divisions at Headquarters shall appoint in writing an ADPSSO for each Standard Workstation system under their individual command. The ADPSO shall be notified of the assignment of ADPSSOs. It is acceptable for one ADPSSO to be responsible for multiple Standard Workstation systems. it is also acceptable, and recommended, that the system manager be appointed ADPSSO provided the system manager duties are not performed by a contractor. The ADPSSO is responsible for implementing the requirements of the AIS Security Manual, this Handbook and any local requirements initiated by the ADPSO. The ADPSSO should have a clearance/background investigation appropriate for the highest sensitivity level of information processed by the system.
2. System Classification/Sensitivity Level. The ADPSSO, in coordination with the official having command responsibility for the system and the ADPSO, shall designate each Standard Workstation system as either classified (Level I) or sensitive (Level II) based on the sensitivity and criticalness of information processed. No Standard Workstation system shall be designated non-sensitive (Level III).

- 2.C.3. AIS Security Plan. The ADPSSO shall prepare a written AIS Security Plan for the activity. The contents of the plan are:
- a. A brief statement of the activity's security policy;
  - b. A narrative description of the Standard Workstation system--it's configuration (may be a diagram), purpose and use;
  - c. A discussion of the application systems processed on the system and the classification/sensitivity level of the data;
  - d. Status on the progress of completing the accreditation process including dates of risk assessments performed, dates of contingency plans, and dates of accreditation;
  - e. A status of personnel security and the progress towards obtaining proper clearances as required;
  - f. A brief discussion of the activity's security awareness and training program; and
  - g. The planned security initiatives for the up-coming year.
  - h. This plan shall be approved by the official having command responsibility for the Standard Workstation system and a copy forwarded to the ADPSO. The plan shall be updated annually. Enclosure (2) contains a sample AIS Security Plan.
4. Risk Assessment. A risk assessment shall be conducted at least every five years for each Standard Workstation system. The Standard Workstation Risk Assessment Methodology (STRAM) shall be used. This methodology requires the ADPSSO to complete an "End User Survey" and the ADPSO to perform the security analysis.
- a. End User Survey. A security survey, called an End User Survey, contains a list of controls which may be in place to protect a Standard Workstation system. These controls are countermeasures to predetermined vulnerabilities (threats) which affect the security posture of Standard Workstations. The ADPSSO completes a survey for each Standard Workstation system by indicating the countermeasures which are in place at the time of the survey. Normally, the ADPSSO can complete a survey based solely upon first-hand knowledge. The end user survey will be supplied to the ADPSSO by the ADPSO.
  - b. Security Analysis. The ADPSO performs an analysis of a system using the information contained in the End User Survey. Upon completion, the ADPSO will have a database with the security profile of the entire command. Most reporting requirements can be satisfied from this database reducing future workload.
  - c. Management Report. A management report is generated as part of the security analysis. It recommends security countermeasures which should be implemented by the activity.

2.C.5. Contingency Plan. A contingency plan shall be prepared by the ADPSSO for each Standard Workstation system. Enclosure (3) contains a sample contingency plan set. Included in this sample plan set is a "starter set" of emergency response actions. This sample contingency plan set should be customized by the ADPSSO. It is understood one contingency plan can be applicable to multiple Standard Workstation systems within the activity. Do not replicate the contingency plan just so "each Standard Workstation system" has its "own" plan. A copy of the plan shall be maintained on the Standard Workstation system and updated annually. At least two printed copies shall be maintained, one stored on-site for easy access and the second stored off-site for access if the other copy is destroyed or cannot be reached during an emergency. The title "Contingency Plan" is generic and actually covers several different areas. Information for these areas could already exist at the unit under a different name such as Emergency Response Plan or Emergency Action Plan, Disaster Recovery Plan, Standard Operating Procedures, Continuity of Operation Plan, etc. Whatever the name, the contingency plan must address action/procedures to be taken in four areas:

- a. Emergency Response. Something out of the norm occurs and an action is required. For example:
    - (1) Event. Power outage occurs during peak operation of heating or air conditioning.
    - (2) Action. Contact building maintenance or unit electrician to reset breaker switches or do it yourself if authorized.
  - b. Backup Operations. Normal operations have been disrupted and temporary processing needs to be initiated. Processing might resume by using another Standard Workstation cluster and loading data from backup floppy diskettes. Processing might also take the form of pen and paper or the typewriter.
  - c. Disaster Assessment. How bad was the disruption? Can normal operations be restored and if so, when? What is the impact to the unit? Does new equipment need to be obtained or office space leased or can data just be restored.
  - d. Recovery Actions. Actions taken to restore normal operations. At some point during this phase data could be restored. Restoration can only happen if backups were taken on schedule and are available from off-site storage (see chapter 3, paragraph C. of this handbook).
6. Security Test and Evaluation (ST&E). An ST&E is necessary for each Standard Workstation system to prove the validity and integrity of the security measures in place. Because of the large number of Standard Workstation systems in the Coast Guard it is not feasible to train ADPSSOs in conducting ST&Es.

- 2.C.6. (cont'd) The evaluation process for the Standard Workstation will be conducted as part of administrative/operational inspections of the activity. Standard Workstation systems may be accredited without a ST&E. If a Standard Workstation system fails the administrative/operational inspection it must be re-accredited.
7. Accreditation Letter/Memo. The ADPSSO shall request accreditation from the DAA. Along with the request the ADPSSO shall provide a copy of the security plan, risk assessment report, and a copy of the contingency plan. An accreditation letter/memo shall be prepared by the ADPSO for each Standard Workstation system after the documentation is reviewed. The ADPSO shall forward the accreditation letter/memo to the DAA along with a recommendation on whether or not the system should be accredited. Each Standard Workstation system must be re-accredited at least every five years. Enclosure (4) contains a sample letter and memo of accreditation.
8. Re-accreditation. Re-accreditation is required at least every five years. However, a Standard Workstation system shall be re-accredited if any of the following occurs:
- a. Change in system managers;
  - b. Major change in system hardware or software;
  - c. Change in the classification/sensitivity level of data on the system; or
  - d. Failure to pass the ST&E (administrative/operational inspection).
9. Interim Authority to Operate. Unclassified Standard Workstation systems not accredited may operate only if an interim authority to operate is issued by the official having command responsibility for the system. An interim authority to operate a classified system may only be granted by the applicable DAA. An interim authority to operate is not a waiver of the requirement for accreditation and is valid for only one year. The interim authority to operate permits an activity to meet its operational mission requirements while completing the accreditation process.

2.D. OTHER STANDARD WORKSTATION SECURITY REQUIREMENTS.

1. Classified Processing. All Standard WorkStation systems used to process classified information shall comply with the following:
  - a. Chapter 18, "Classified Information Processing," of COMDTINST M5500.13 series, AIS Security Manual;
  - b. COMDTINST S2241.5 series, Tempest Policy and Tempest Countermeasures for Shore Facilities;
  - c. COMDTINST M5510.4 series, Shipboard Design, Installation and Red/Black Engineering Criteria for Secure Electrical Information Processing Systems;
  - d. COMDTINST M5500.11 series, Security Manual.
  - e. If a Standard Workstation system is used for classified processing the hard disk becomes classified material and cannot be declassified or cleared through existing methods. Standard Workstation hard disks which have intentionally or unintentionally become classified shall be secured and controlled as classified material. A hard disk which becomes inoperable may be removed by maintenance personnel who do not have a clearance under the following conditions:
    - (1) No maintenance is performed except in the presence of Coast Guard personnel who have a clearance at least as high as the highest classification level of information on the hard disk;
    - (2) The Coast Guard personnel present ensure maintenance personnel do not access the hard disk; and
    - (3) Coast Guard personnel maintain custody of the classified hard disk until it is declassified or destroyed in accordance with the AIS Security Manual.
2. Personnel Security.
  - a. Personnel using a Standard Workstation system shall have their billets or positions designated in terms of ADP sensitivity. See Chapter 6, "Personnel Security," of the AIS Security Manual.
  - b. Military, civilian, and contractor personnel who will be involved in classified or sensitive computer operations and who will occupy positions designated ADP sensitive, shall have an appropriate clearance or background investigation (Note: All U.S. Government civilian and military employees have had, at a minimum, the appropriate background investigation for the sensitivity level ADP-I (Non-sensitive) positions).
  - c. When dealing with military personnel the activity's Security Manager can provide assistance. When dealing with civilian or contractor personnel contact the activity's civilian personnel office.

- 2.D.3. Security Awareness and Training. The ADPSO shall establish for the command and the ADPSSO shall establish for the activity a security awareness and training program. This program will assure Coast Guard and contractor personnel involved in the management, operation, programming, maintenance, or use of Standard Workstation systems are aware of their security responsibilities and know how to fulfill them. Commandant (G-TIS-3) will provide the curricula and material to the ADPSO for distribution.
4. Self-Audit Report. The ADPSO shall send Commandant (G-T) a consolidated AIS Security Program Self-Audit Report RCS-TIS-16232 (previously known as RCS-G-TDS-16232), which summarizes accreditation progress for the command and all its subordinate activity's. This report is submitted to Commandant (G-TIS-3) no later than 30 June of each year (see Chapter 15, "AIS Security Documentation Requirements," of the AIS Security Manual). These reports will contain sensitive information about the security posture of an activity and should be handled accordingly.
5. Sensitive Application Certification. Each sensitive application (see definitions, chapter 1, paragraph C.7 of this manual) shall be developed in accordance with the Sensitive Application Design Guide (SADG) and certified every 3 years using the Sensitive Application Certification (SAC) Methodology. This process is described in Chapter 14 of the AIS Security Manual and the SAC Methodology. Most sensitive applications in the Coast Guard are developed for support of Coast Guard programs managed by Headquarters (i.e., MSIS, PMIS/JUMPS, ARMS, etc.). The review of these Coast Guard-wide sensitive applications will be coordinated by Commandant (G-TIS). A few sensitive applications, which are unique to an area office, district office, or Headquarters unit, may be developed. If a command develops a sensitive application then that command is responsible for the review of the application. It is not expected that other activities, such as a group or unit, would develop sensitive applications. In the rare case where one of these activities did develop a sensitive applications, the activity would be responsible for the review (NOTE: Activities who use a sensitive application developed by another activity, such as an MSO using MSIS, or a unit which inputs data to an application unique to a district, are not responsible for the review of the sensitive application system. However these user activities should cooperate with the developer of the sensitive systems in any review.).

## CHAPTER 3. SECURITY CONTROLS

- A. GENERAL. Security features incorporated in the Standard Workstation system are limited; those security features that exist, such as password protection, are provided in software. Although passwords and various protection levels can be specified at the volume, directory and/or file level, additional precautions must be taken to ensure the protection of sensitive applications and files.
- B. PHYSICAL CONTROLS.
  - 1. Physical Access. Standard Workstation equipment should be located in areas which can be locked during non-work hours. Physical protection is particularly important for Standard Workstations which have floppy or hard disks and can be used to initialize or load the operating system.
  - 2. Logout. Workstations shall be logged-out when not in use or unattended. Workstations shall not remain in any utility or application (word processing, Multiplan, etc.) which can terminate in the executive mode when unattended.
  - 3. Workstation Placement. Workstations which will be used to process sensitive information should be located to discourage over-the-shoulder browsing and should not be located where they are visible from outside the working space (e.g., windows, passageways).
- C. ADMINISTRATIVE CONTROLS.
  - 1. System Usage.
    - a. System Managers and ADPSSOs must know what sensitivity level and type of data users have on the system. An inventory shall be kept of sensitive applications.
    - b. Procedures shall be developed for non-work hour access to the Standard Workstation system so an audit trail exists of all persons using the system at these times. Written procedures should be incorporated into a general SOP for the Standard Workstation.
  - 2. Backup. The ADPSSO should ensure a recurring backup schedule of at least once a week for essential system resident files. Users should be encouraged to backup their critical files to floppy diskettes (or other media) more frequently.
  - 3. Backup storage. There should be two copies of each backup: one for on-site storage and the second for off-site storage. One copy should be protected in a locked cabinet or safe on-site. Fireproof containers are recommended. Whenever possible this storage area should be located away from the Standard Workstation system. If the backups are in a different area and a catastrophe (fire, flood, etc.) occurs to the system the risk of damage to backups would be reduced.

- C. 3. (cont'd) Portable floppy diskette storage boxes, even though lockable, provide inadequate protection when left out on a desk or in plain view of passersby. A second copy of each backup should be stored off-site. An off-site storage facility equipped for storing magnetic media is preferred but may not be feasible. Some Federal Records Centers are equipped for such storage free of charge as well as commercial facilities. If an FRC is not convenient, especially for emergency retrieval, a commercial facility, another building on base, or another Coast Guard activity may meet the need for off-site storage. The ADPSSO should require more than one "generation" of backups are maintained. If the example backup scheme (shown below) is continued, files that are three weeks old can be recovered. Example:  
commercial
- a. The first week Backup "A" is done;
  - b. The second week Backup "B" is done, Backup "A" is retained;
  - c. The third week Backup "C" is done, Backups "A" and "B" are retained;
  - d. The fourth week Backup "A" is overwritten with a new backup "A", Backups "B" and "C" are retained;
4. Passwords. Password protection is the primary security feature of the Standard Workstation. There are three types of passwords - volume password, directory password, and file password. Directory and file passwords have different levels of protection which may be used to meet different needs. The standard Workstation documentation contains the current password levels and the protection each affords. The password scheme is an integral part of the software system and cannot be readily changed without significant impact on the operating system, individual software applications and utilities. Since the typical user, who is not a trained data processor, might easily stumble upon the volume password, the following procedures shall be followed.
- a. All Standard Workstation systems shall require signon passwords to access the system. Each user shall have a signon password. If Electronic Mail is in use, System Managers should activate passwords for users, since directory and Electronic Mail passwords must be in "sync."
  - b. The ADPSSO should educate users about password creation and protection.
    - (1) The recommended method for the development of a password is to take a group of words or phrases familiar to the user and combine all or portions of them to form the password. Passwords shall be no less than six (6) alphanumeric characters to minimize the risk of passwords being guessed. For example: the password EVOTTUPA is derived from the phrase, "EVery OTHER TUESday is PAYday" and can be easily memorized. Passwords based on family member names, initials, birthdays, etc. can be easily guessed and should be avoided.

- C. 4. b. (2) Users should not write down passwords or reveal them to others in any way. If data must be shared among several people, it should be placed in a common directory and only those who have a need to access the data should be given the password.
  - c. System Managers should have two User IDs and two unique passwords - one for system administration duties and a second User ID for daily work. The volume password should be known by the system manager and one alternate. It should be written down, sealed in an envelope, and stored in a secure location for emergency use if the system manager and alternate are not available. The volume password shall only be given to those who have an absolute need to know it.
  - d. The volume password shall not be used to signon to any Standard Workstation system except in a emergency.
  - e. System Managers shall change volume passwords (using the change Volume Name command) periodically (quarterly is reasonable). Volume passwords shall be changed with the change of system managers, when anyone who knows the volume password no longer needs access to the system, and if it becomes known that the volume password has been compromised. The volume password should also be changed using the Change Volume Name command immediately after initializing a volume. These are added precaution to keep the volume password from being discovered.
  - f. System Managers shall change user passwords periodically (semiannually is reasonable).
5. Application/Utility Access. System Managers should ensure users are provided executive command sets based on need-to-know criteria. System managers should customize command sets for various user communities. In some cases it may be appropriate to limit a user to only one application, such as word processing. The following commands should be reserved for the System Manager's command set only: "Command File Editor", "User File Editor", "Dump", "New Command", "Remove Command", "Debug File", "Set File Protection", and "Set Directory Protection". See enclosure (4) for examples of customized user command sets.
6. Volume/Directory/File Protection.
- a. System files not required by general users should be protected at the "O" level to prevent viewing/analysis by unauthorized personnel. System files such as "fileheaders.sys," "mfd.sys," and "name.users" are particularly sensitive in that the user's directory or mail passwords may be identified.

- C. 6. b. When a floppy diskette is initialized the password (either volume or directory) invoked for the user's current path is passed to [f0]<sys>fileheaders.sys file and can easily be determined. The floppy (volume) should be password protected or the path command used to change the current password to a null password (two single quotes ['']) prior to initializing the floppy.
- c. When using the "Copy" command to copy a document from one directory to another, the password associated with the source document is written to the new document in the fileheaders.sys file. Always assign a new password to the new document using "^newdocument password" after the new document name in the "file to" parameter.
- d. If there is any reason to question the confidentiality or integrity of a file, the System Manager should review system data to determine if the file has been accessed at an unusual time (e.g., off duty hours or at a time not coincident with the normal processing cycle). The "Files" command can provide information regarding last date/time of file modification. The word processing "List" command can provide information regarding last date/time of file access. System Managers should advise owners of sensitive files to review their own files for compromise.
- 7. Software Licenses. Computer programs (software) are the property of their creators, similar to the copyrighting of books. The exception is programs which have been released to the public domain. When a program is purchased, the user obtains a license to use the program. Normally the license does not permit copying or further distribution of the program. Nonetheless, "bootleg" or pirated copying of programs has become a worldwide problem. It amounts to the theft of the software. All software shall be operated in compliance with its licensing agreement. No unauthorized copies or further distribution of software shall be made.
- 8. Public Domain Software. There has been an increasing number of instances in which public domain software has damaged hardware, software, and data on computer systems. Public domain software is prohibited from being installed and used on any Coast Guard computer system unless it is a Coast Guard product or written authorization is obtained from the official having command responsibility for the system.
- 9. Individual Use of Standard Workstations. Standard Workstation systems are installed to conduct Coast Guard business. By their nature, their capabilities are subject to diversion for personal use. Some systems come programmed for recreational use (electronic games such as RATS). The following procedures shall be followed.
  - a. Games. Video games are not authorized.
  - b. Mail. Electronic mail is subjected to the same "official use only" constraints as government mail or telephone.

- C. 9. c. Personal Use. Personal use is prohibited; systems may be used for government business only.
- d. Training. Personnel are encouraged to learn the capabilities of the installed systems by working "hands on" projects such as composing a letter in word processing. This effort should constitute training, familiarization, or actual accomplishment of Coast Guard business. Diverting the systems into private projects is not authorized.
- C. 10. Miscellaneous.
  - a. ADPSSOs should ensure System Managers promptly remove system access rights for any person no longer requiring access.
  - b. Sigon procedures (including passwords) should not be posted on or around the Standard Workstation or office spaces.
  - c. In certain modes of operation the Standard Workstation operating system does not mask a password (i.e., replace with "#" symbols). For example, when using the Asynchronous Terminal Emulator (ATE) or Multi-Terminal Emulator (MTE) mode to communicate with TCC's AMDAHL mainframe, the AMDAHL password is not masked and remains visible on the Standard Workstation screen until it is scrolled off. Users should use care when entering passwords while in these modes to prevent unauthorized viewing of a password.
  - d. ADPSSOs should ensure, if possible, that Standard Workstation equipment used to process unclassified sensitive information is "cleansed" of all sensitive data before it is returned for repair or traded within the USCG. For sensitive but unclassified systems initializing the disk or deleting all sensitive files using the security option will be adequate.
  - e. Floppy diskettes which contain sensitive information and need to be discarded (e.g., due to excessive bad spots/defects) should be shredded or degaussed.
  - f. External communications links should be disconnected during offduty working hours unless approved by the ADPSSO for operational needs (e.g. electronic mail, PMIS, etc.).

**SAMPLE**

**AIS SECURITY PLAN**

**INFORMATION SYSTEMS DIVISION**

30 JUNE 1988

Submitted by:	R. N. Karr	Date:	30 June 1988
Reviewed by:	M. P. Kane (ADPSO, Acting)	Date:	30 June 1988
Approved by:	CAPTAIN R. J. Offutt, Jr. (G-TIS)	Date:	30 June 1988

**AIS SECURITY PLAN**

**INFORMATION SYSTEMS DIVISION (G-TIS)**

- A. PURPOSE. The Information Systems Division (G-TIS) Automated Information Systems Security Plan (AISSP) provides security policies; a description of Automated Information Systems (AISs) and the security environment in G-TIS; a description of AIS security responsibilities; and a schedule which summarizes events leading to system accreditation.
  
- B. SCOPE. This Security Plan is in accordance with the AIS Security Manual (COMDTINST M5500.13A). It applies to all ADP systems, Office Information Systems (OISs), and telecommunications networks operated under the following conditions:
  - 1. In support of or on behalf of G-TIS.
  - 2. Those systems electrically connected to a host ADP/OIS system under control of G-TIS. This includes those systems/networks/terminals operated by commands having access via a public or private packet switching communications network.
  
- C. AIS SECURITY OBJECTIVES.
  - 1. To provide an organized approach to AIS security.
  - 2. To ensure that all data handled by ADP systems, office information systems, and telecommunications networks are adequately protected against accidental or intentional destruction, modification, or disclosure of data, and users are protected against denial of service.
  - 3. To ensure that countermeasures applied to achieve AIS security are cost-effective.
  - 4. To provide security awareness training to all G-TIS personnel using division AISs.
  
- D. POLICY STATEMENT.
  - 1. Information is a Coast Guard resource; it will be protected for Privacy or other purposes as needed. It will be made available to only those who have a valid need-to-know.
  - 2. G-TIS personnel will comply with the policy, responsibilities, and requirements in this Plan and in the AIS Security Manual (COMDTINST M5500.13A) to protect USCG information and information processing facilities.
  - 3. All G-TIS personnel will be provided orientation regarding the use and protection of Coast Guard information by the Automated Data Processing Security Officer (ADPSO).

Encl (1) to COMDTINST M5500.17

4. A risk assessment of G-TIS AISs will be conducted every five years or whenever major changes to hardware, software, AIS facilities, or other such events may affect a system's security posture or upon change of system manager. A schedule for risk assessments is contained in enclosure (3).
5. Sensitive application systems will be certified every three years or whenever major changes to software may affect a system's security posture or upon change of application manager. A schedule of system certifications is contained in enclosure (3).
6. A written Contingency Plan shall be prepared and maintained by the ADPSO (G-TIS-5). This plan may be included in G-TIS Standard Operating Procedure(s).
7. Automated Data Processing System Security Officer(s) (ADPSSOs) and system manager(s) shall be appointed for each system within G-TIS and designated in writing to the ADPSO.
8. Compliance with security measures shall be part of the ADPSSO's and system manager's critical job elements (CJE)/officer's evaluation report (OER). The system manager will be evaluated annually on compliance/performance of AIS security measures.

E. AIS ENVIRONMENT.

1. The following information systems, described in detail in enclosure (1), are covered by the G-TIS AIS Security Program and this plan.

<u>System</u>	<u>OPFAC NO.</u>
a. Standard Workstation Cluster (G-TIS)	98-70015
b. Information Center Administrative Cluster (G-TIS-5)	98-70015
c. Information Center Training Cluster (G-TIS-5)	98-70015
d. Information Center Video Cluster (G-TIS-5)	98-70015
e. Data Administration IBM PC (G-TIS-4)	98-70015
f. Information Center Apple Macintosh (G-TIS-5)	98-70015
g. Data 100 (G-TIS-5)	98-70015

2. G-TIS shall have an on-going security awareness program supplemented by security video tapes available through the Information Center.

F. AIS SECURITY ORGANIZATION AND RESPONSIBILITIES.

1. G-TIS personnel having direct responsibility for managing or implementing security within the division include:
  - a. G-TIS: Issues policy.

- b. G-TIS-3: Serve as Acting ADPSO for the Office of Command, Control, and Communications. The role of Acting ADPSO is expected to end February 1989.
  - c. G-TIS-5: Function as ADPSO For the Office of Command, Control and Communications. Responsibility will be assumed upon accreditation of G-TIS (Scheduled for February 1989).
  - d. ADPSSO(s)/System Manager(s): Comply with requirements of this Plan and those contained in the AIS Security Manual, COMDTINST M5500.13A. Execute security measures and practices as issued by the G-T ADPSO.
- 2. The responsibilities of G-TIS, the ADPSO, and the ADPSSO(s) are contained in COMDTINST M5500.13A, Chapters 2 and 15.
  - 3. The ADPSSO serves as the G-TIS staff advisor in matters of AIS security. He ensures G-TIS-wide performance of the duties specified in COMDTINST M5500.13A, Chapters 2 and 15, including developing, implementing, and maintaining this Plan; updating system security survey's; coordinating and/or participating in risk assessments, sensitive application certifications, security test and evaluations, and contingency plan development; coordinating the preparation and maintenance of accreditation support documentation as directed by the (G-T) ADPSO. The ADPSSO will also ensure that all AIS security incidents or violations are investigated, documented, and reported.
  - 4. G-TIS billets and positions have been reviewed in accordance with COMDTINST M5500.13A, Chapter 6, to determine appropriate ADP clearances. A list of G-TIS billets and positions having clearance levels ADP III and II are listed in enclosure (2). All other billets and positions have been designated as ADP I. All personnel assigned to billets or positions listed in enclosure (2) shall receive the necessary personnel clearance for their assignment.
- G. AIS ACCREDITATION SCHEDULE. Enclosure (3) is the proposed accreditation schedule for G-TIS.
- H. ENCLOSURES.
- 1. Automated Information Systems List.
  - 2. G-TIS Billet/Position Clearances.
  - 3. Activity AIS Accreditation Schedule.

**INFORMATION SYSTEMS DIVISION**

**AUTOMATED INFORMATION SYSTEMS LIST**

System security survey's have been completed for each of the following systems and are on file with the ADPSO. Those with a "need to know" should contact the ADPSO, G-TIS-5.

1. ACTIVITY NAME : G-TIS  
SYSTEM NAME : Standard Workstation Cluster  
ADPSSO : LT D. Jones, G-TIS-5, (202) 267-1280  
CT-MAIL ADDRESS: G-TIS-5
2. ACTIVITY NAME : G-TIS  
SYSTEM NAME : Information Center Administrative Cluster  
ADPSSO : LT-D. Jones, G-TIS-5, (202) 267-1280  
CT-MAIL ADDRESS: G-TIS-5
3. ACTIVITY NAME : G-TIS  
SYSTEM NAME : Information Center Training Cluster  
ADPSSO : LT D. Jones, G-TIS-5, (202) 267-1280  
CT-MAIL ADDRESS: G-TIS-5
4. ACTIVITY NAME : G-TIS  
SYSTEM NAME : Information Center Video Cluster  
ADPSSO : LT D. Jones, G-TIS-5, (202) 267-1280  
CT-MAIL ADDRESS: G-TIS-5
5. ACTIVITY NAME : G-TIS  
SYSTEM NAME : Data Administration IBM PC  
ADPSSO : B. Price, G-TIS-4, (202) 267-1316  
CT-MAIL ADDRESS: G-TIS-4
6. ACTIVITY NAME : G-TIS  
SYSTEM NAME : Information Center Apple Macintosh  
ADPSSO : LT D. Jones, G-TIS-5, (202) 267-1280  
CT-MAIL ADDRESS: G-TIS-5
7. ACTIVITY NAME : G-TIS  
SYSTEM NAME : Data 100  
ADPSSO : LT D. Jones, G-TIS-5, (202) 267-1280  
CT-MAIL ADDRESS: G-TIS-5

Encl (1) to COMDTINST M5500.17

ENCLOSURE 2

**INFORMATION SYSTEMS DIVISION**

**G-TIS BILLET/POSITION CLEARANCES**

This information is maintained by the Classified Material Control Officer (CMCO), LT F. Polk, G-TIS-2. The position clearances and clearance levels are reviewed annually.

ACTIVITY AIS ACCREDITATION SCHEDULE'

1. ORGANIZATION NAME AND ADDRESS  
 a. NAME: INFO AYS DIV (G-TIS)  
 b. ADDRESS: 2100 2ND STREET. S.W.  
WASHINGTON. D.C. 20593

2. CO'S NAME AND TELEPHONE  
 a. NAME: CAPTAIN J.R. OFFUTT. JR.  
 b. FTS: 267-1463  
 c. COMMERCIAL: SAME

3. DPSO'S NAME AND TELEPHONE  
 a. NAME: M. KANE. ACTING  
 b. FTS: 267-1324  
 c. COMMERCIAL: SAME

ACTIVITY AIS DATA					ESTIMATED SCHEDULE				
4	5	6	7	8	9	10	11	12	13
	AIS	AIS	DATA	APPLICATION NAME					ADPSSO
DAA	OPFAC	SYSTEM	LEVELS	(LEVELS II & III ONLY)	RA	CP	CERT	ACCRED	OR OISSO
	NUMBER	NAME	I-II-III						NAME
G-T	98-70015	STANDARD WORKSTATION	II, III		01/88	08/88	01/89	02/89	G-TIS-5
		CLUSTER (G-TIS)							
G-T	98-70015	Information Center Admin	II, III		01/88	08/88	01/89	02/89	G-TIS-5
		Cluster (G-TIS-5)							
G-T	98-70015	Information Center Train	III		01/88	08/88	01/89	02/89	G-TIS-5
		Cluster (G-TIS-5)							
G-T	98-70015	Information Center video	III		01/88	08/88	01/89	02/89	G-TIS-5
		Cluster (G-TIS-5)							
G-T	98-70015	Data Administration IBM	III		10/88	08/88	01/89	02/89	G-TIS-4
		PC (G-TIS-4)							

(Use additional sheets if needed)

Encl (1) to COMDTINST M5500.17

ENCLOSURE 3 (Con't)

ACTIVITY AIS ACCREDITATION SCHEDULE

1. ORGANIZATION NAME AND ADDRESS  
 a. NAME: INFO SYS DIV (G-TIS)  
 b. ADDRESS: 2100 2ND STREET. S.W.  
WASHINGTON. D.C. 20593

2. C'Os NAME AND TELEPHONE  
 a. NAME: CAPTAIN J.R. OFFUTT. JR.  
 b. FTS: 267-1463  
 c. COMMERCIAL: SAME

3. ADPSO'S NAME AND TELEPHONE  
 a. NAME: M. KANE, Acting  
 b. FTS: 267-1324  
 c. COMMERCIAL: SAME

ACTIVITY AIS DATA					ESTIMATED SCHEDULE				
4	5	6	7	8	9	10	11	12	13
	AIS	AIS	DATA	APPLICATION NAME					ADPSSO
	OPFAC	SYSTEM	LEVELS	(LEVELS II & III ONLY	RA	CP	CERT	ACCRED	OR OISSO
	NUMBER	NAME	I-II-III						NAME
G-T	98-70015	Information Center Apple Macintosh (G-TIS-5)	III		10/88	08/88	01/89	02/89	G-TIS-5
G-T	98-70015	Data 100 (G-TIS-5)	II. III		01/88	08/88	01/89	02/89	G-TIS-5

(Use additional sheets if needed)

Encl (2) to COMDTINST M5500.17

**SAMPLE**  
**CONTINGENCY PLAN SET**  
**FOR THE**  
**UNITED STATES COAST GUARD**  
**STANDARD WORKSTATION CLUSTER SYSTEM**

Encl (2) to COMDTINST M5500.17

**SAMPLE**  
**EMERGENCY RESPONSE**  
**FOR THE**  
**STANDARD WORKSTATION CLUSTER SYSTEM**  
**UNITED STATES COAST GUARD**  
**INFORMATION SYSTEMS DIVISION**

08/10/88

COPY NO. \_\_\_\_\_

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1.0 INTRODUCTION . . . . .	1
1.1 Fire. . . . .	2
1.2 Water Damage. . . . .	3
1.3 Power Failure . . . . .	4
1.4 Communications Failure. . . . .	5
1.5 Air Conditioning Failure. . . . .	6
1.6 System Hardware Failure . . . . .	7
1.7 Personnel Accident/Injury . . . . .	8
1.8 Bomb Threat . . . . .	9
1.9 Software Failure. . . . .	10
1.10 Illegal/Unauthorized Entry. . . . .	11
1.11 Theft . . . . .	12
1.12 Inclement Weather . . . . .	13
1.13 Explosion . . . . .	14
1.14 Public Emergency/Civil Disorder . . . . .	15
2.0 ENCLOSURE (S)	
Emergency Response Team Members . . . . .	16

Encl (2) to COMDTINST M5500.17

## 1.0 INTRODUCTION

This document details emergency responses to be taken by **G-TIS** personnel in the event of an emergency situation which affects the **Standard Terminal Cluster** system facility. The objective of the emergency response is to prevent or minimize injury/damage to personnel and/or to the **Standard Terminal Cluster** system.

Enclosure 1 lists the members of the Emergency Response Team for the **Standard Terminal Cluster** system. This list shall be used as the emergency contact list in the event of an emergency situation. The information on the following pages is presented in the following format.

- o Event.
- o Objective(s).
- o Actions to be taken during scheduled work hours.
- o Actions to be taken during off-duty hours.

Encl (2) to COMDTINST M5500.17

1.1 **EVENT: Fire**

**OBJECTIVE(S) :**

1. Protect lives and ensure safety of facility personnel. **UNDER NO CIRCUMSTANCES WILL ANYONE SUBJECT THEMSELVES OR THEIR SUBORDINATES TO DEATH OR INJURY TO PROTECT THESE MATERIALS FROM FIRE.**
2. Minimize damage to data and facility resources associated with the **Standard Terminal Cluster** system.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Engage Emergency Power Off (EPO) located near the Data Terminal Center exit.
2. If fire is visible and localized (e.g. a trash can fire) and fire alarm has not sounded:
  - a. Disable Halon system at control panel in the Data Terminal Center.
  - b. Attempt to extinguish fire using hand held fire extinguishers located in computer room
  - c. If fire cannot be put out immediately - enable fire alarm and Halon system at control panel in the Data Terminal Center.
3. Evacuate the Data Terminal Center, closing all doors when leaving.
4. Contact guard office (see enclosure 1 for contact information) from nearest phone, giving following information:
  - a. Your name and physical location.
  - b. Location of fire and other description of fire, such as type, size.
  - c. Specify that the Data Terminal Center is evacuated, or other status.
5. Proceed to nearest exit to street, or designated meeting location.
6. Notify Chief or Assistant Chief, Information Systems Division and Chief, Information Center (ADPSO) of event and any actions taken. See enclosure 1 for contact information.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.

\* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

**OBJECTIVE (S) :**

1. Minimize damage to data, electronic equipment and other facility resources.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Engage Emergency Power Off (EPO) switch if water endangers electronic components.
2. If water source is overhead, cover equipment with water repellent tarpaulins or plastic covers.
3. Notify Chief, Facilities Branch (G-CAS-2). See enclosure 1 for contact information.
4. Notify Assistant Chief, Information Systems Division and Chief, Information Center (ADPSO) of problem. See enclosure 1 for contact information.
5. Move material (e.g. media, supplies) that may be affected by water to elevated positions or to alternate storage location.
6. Evacuate area if necessary.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

Encl (2) to COMDTINST M5500.17

**1.3 EVENT: Power Failure**

**OBJECTIVE(S) :**

1. Minimize damage to electronic components and data stored on them.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Engage Emergency Power Off (EPO) switch.
2. Turn off all individual power switches on electronic components.
3. Notify Chief, Facilities Branch (G-CAS-2). See enclosure 1 for contact information.
4. Notify Chief, Information Center (ADPSO). See enclosure 1 for contact information.
5. Ensure all individual power switches remain in OFF position until power is returned and determined by the Chief, Facilities Branch (G-CAS-2) to be stable.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

1.4 **EVENT:** Communications Failure (CT-Mail, ATE, MTE, Cable Break, etc.)

**OBJECTIVE (S) :**

1. Minimize duration and affects of loss of communications links.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Notify the System Manager. See enclosure 1 for contact information.
2. If communications failure impacts production run (i.e. critical deadline job) notify Chief, Information Center (ADPSO) of such impact. See enclosure 1 for contact information.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.

\* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

Encl (2) to COMDTINST M5500.17

1.5 **EVENT: @Air Conditioning Failure**

**OBJECTIVE(S) :**

1. Minimize/prevent damage to electronic components.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Notify Chief, Facilities Branch (G-CAS-2) of problem. See enclosure 1 for contact information.
2. Notify Chief, Information Center (ADPSO). See enclosure 1 for contact information.
3. If temperature exceeds 80 degrees in computer room:
  - a. Notify users and power down **Standard Terminal Cluster** system.
  - b. Station personnel at doorway and open door to dissipate heat.
  - c. If temperature returns to acceptable level, system can be operated until the temperature again exceeds 80 degrees.
4. If temperature remains above 80 degrees, or doors are not to be opened, **Standard Terminal Cluster** system should remain off until A/C is operable.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

1.6 **EVENT:** System Hardware Failure

**OBJECTIVE (S) :**

1. Minimize system downtime; prevent damage to electronic components, application/system software.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. If hardware component has alternate backup device, switch to alternate backup device.
2. Attempt to recover failed hardware component (e.g. cold start.
3. If attempt successful, continue processing.
4. If attempt unsuccessful:
  - a. Power down failed unit
  - b. Notify the System Manager of component status. See enclosure 1 for contact information.
  - c. If component failure impacts production run (i.e. critical deadline job) notify Chief, Information Center (ADPSO) of such impact.

**ACTIONS TO BE TAKEN OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

Encl (2) to COMDTINST M5500.17

1.7 **EVENT:** Personnel Accident/Injury

**OBJECTIVE(S) :**

1. Minimize risk to life, provide aid to injured personnel.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Do not move injured person; provide first aid if possible.
2. Notify First Aid Officer and/or Clinic. See enclosure 1 for contact information.
3. Notify Assistant Chief, Information Systems Division and Chief, Information Center (ADPSO). See enclosure 1 for contact information.
4. Notify Safety Officer. See enclosure 1 for contact information.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

1.8 **EVENT:** Bomb Threat

**OBJECTIVE (S) :**

1. Protect lives, minimize damage to electronic components and facility resources.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Remain calm, be courteous, and listen; do not interrupt the caller. Immediately request the nearest person, by note, to advise the Commanding Officer that you are receiving a bomb threat call. Write out the caller's message in its entirety. See enclosure 1 for contact information.

If the caller seems agreeable to further conversation, ask questions like:

- o When will it go off? Hour? Time Remaining?
- o Where is it located? Floor? Area?
- o Has the bomb been placed in the open?
- o How is it disguised?
- o How is it concealed?
- o What type and size of bomb?
- o How did it get into the building? Mailed or carried?
- o How do you know so much about the bomb?
- o What is your name and address?

2. Call Guard Office and relate threat conversation. See enclosure 1 for contact information.
3. Notify Chief, Facilities Branch (G-CAS-2). See enclosure 1 for contact information.
4. If instructed to evacuate (see enclosure 1 for contact information) by Commanding Officer:
  - a. Execute Emergency Power Off (EPO) and secure the computer room
  - b. Evacuate computer room and building.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

Encl (2) to COMDTINST M5500.17

1.9 **EVENT:** Software Failure

**OBJECTIVE(S) :**

1. Minimize damage/loss of data and system availability.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Attempt to restart job.
2. If attempt successful, continue processing.
3. If attempt unsuccessful:
  - a. Maintain status of system (do not power down).
  - b. Notify the System Manager of system status.
  - c. If failure impacts production run (critical deadline job) notify Chief, Information Center (ADPSO).

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

1.10 **EVENT:** Illegal/Unauthorized Entry to Facility

**OBJECTIVE (S) :**

1. Protect AIS hardware and software.
2. Minimize the risk of damage/loss of data, hardware, and software.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Request identification. Avoid clash with unauthorized entrant.
2. Ask entrant to leave ADP premises - note badge ID.
3. Call Chief, Information Center (ADPSO) or Guard Desk. See enclosure 1 for contact information.
4. Notify Assistant Chief, Information Systems Division. See enclosure 1 for contact information.
5. Move vital data to safer location if necessary.
6. Shut down the **Standard Terminal Cluster** system if unauthorized entry by means of a terminal is suspected.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Member list, enclosure 1 for contacts and phone numbers.

Encl (2) to COMDTINST M5500.17

1.11 **EVENT:** Theft

**OBJECTIVE(S) :**

1. To expedite the recovery or replacement of the missing resource(s).

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Itemize the missing resources.
2. Notify Assistant Chief, Information Systems Division and Chief, Information Center (ADPSO). See enclosure 1 for contact information.
3. Call Guard Desk. See enclosure 1 for contact information.
4. Make assessment of the impact on processing function.
5. Do not touch anything until proper authorities have arrived.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

1.12 **EVENT:** Inclement Weather (Tornado, Hurricane, etc.)

**OBJECTIVE(S) :**

1. To minimize threat /loss to life and/or property.

**ACTION TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Notify Assistant Chief, Information Systems Division and Chief, Information Center (ADPSO). See enclosure 1 for contact information.
2. Contact Chief, Facilities Branch (G-CAS-2). See enclosure 1 for contact information.
3. Move vital data to safer location if required.
4. Evacuate and secure the Data Terminal Center if necessary.
5. Shut down the system using the Emergency Power Off (EPO) switch near the Data Terminal Center exit.

**ACTION TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

Encl (2) to COMDTINST M5500.17

1.13 **EVENT:** Explosion

**OBJECTIVE (S) :**

1. To protect life and property.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Immediately engage Emergency Power Off (EPO) switch and evacuate the Data Terminal Center.
2. Notify Chief or Assistant Chief, Information Systems Division and Chief. Information Center (ADSP0) of status. See enclosure 1 for contact information.
3. Call Guard Desk. See enclosure 1 for contact information.
4. Take roll call of Data Terminal Center personnel and notify the Personnel Movement Officer. See enclosure 1 for contact information.
5. Notify Chief, Facilities Branch (G-CAS-2). See enclosure 1 for contact information.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.
- \* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

1.14 **EVENT: Public Emergency/Civil Disorder**

**OBJECTIVE(S) :**

1. Minimize the threat to life and property.

**ACTIONS TO BE TAKEN DURING SCHEDULED WORKING HOURS:**

1. Call Guard Desk/Office Of Security. See enclosure 1 for contact information.
2. Contact Chief or Assistant Chief, Information Systems Division and Chief, Information Center (ADPSO). See enclosure 1 for contact information.
3. Shut down AIS systems and secure the Data Terminal Center if necessary.

**ACTIONS TO BE TAKEN DURING OFF-DUTY HOURS:**

1. The Data Terminal Center is locked during off-duty hours. Therefore no action can be taken until duty hours resume.

\* See Emergency Response Team Members list, enclosure 1 for contacts and phone numbers.

**SAMPLE**  
**DISASTER ASSESSMENT**  
**FOR THE**  
**STANDARD WORKSTATION CLUSTER SYSTEM**  
**UNITED STATES COAST GUARD**  
**INFORMATION SYSTEMS DIVISION**

08/10/88

COPY NO. \_\_\_\_\_

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1.0 INTRODUCTION. . . . .	1
1.1 Responsibilities of Disaster Assessment Team. . . . .	1
1.1.1 Chief, Information Center (ADPSO). . . . .	1
1.1.2 System Manager . . . . .	2
1.1.3 Chief, Facilities Branch (G-CAS-2) . . . . .	2
1.2 Results of Damage Assessment. . . . .	2
2.0 ENCLOSURE(S)	
Disaster Assessment Team Members. . . . .	3
Standard Workstation Cluster Hardware Inventory . . . . .	4
Standard Workstation Cluster Software Inventory . . . . .	5
Critical System Priority List . . . . .	6
Off-Site Storage Inventory. . . . .	7
Loss Evaluation Sheet(s). . . . .	8
Back-up Storage Inventory . . . . .	9
Memos of Understanding. . . . .	10

## 1.0 INTRODUCTION

The Disaster Assessment Team (Enclosure 1) is composed of **G-TIS** management and supervisory personnel from areas affecting the **Standard Workstation Cluster** system, building maintenance, and user activities. Each individual named to the team has specific knowledge of one or more areas of **G-TIS** operations directly affected by the **Standard Workstation Cluster** system.

The team is notified of the existence of a contingency situation by the Chief, Information Center (ADPSO). The Chief sets a time and place for the Disaster Assessment Team members to meet.

The Disaster Assessment Team's goal is to determine whether to initiate recovery at the **Data Terminal Center**, or if it is necessary to implement off-site backup operations while recovery takes place. The following material is available to the team from the contingency plan:

- o **Standard Workstation Cluster** Hardware Inventory (Enclosure 2).
- o **Standard Workstation Cluster** Software Inventory (Enclosure 3).
- o Critical System Priority List (Enclosure 4).
- o Off-Site Storage Inventory (Enclosure 5).
- o Loss Evaluation Sheets (Enclosure 6).
- o Back-up Storage Inventory (Enclosure 7).
- o Memos of Understanding (Enclosure 8).

Loss Evaluation Sheets are used by the team to assess the extent of physical damage to electronic components of the **Standard Workstation Cluster** system resulting from the emergency situation.

The following section details the responsibilities of each of the members of the Disaster Assessment Team. Guidelines for determining the severity of the disaster and the resultant decisions for recovery of data processing capabilities at **G-TIS** and/or back-up operation at an off-site location are specified.

### 1.1 RESPONSIBILITIES OF DISASTER ASSESSMENT TEAM

#### 1.1.1 Chief, Information Center (ADPSO).

This individual functions as the chairman of the Disaster Assessment Team. He is notified in case of emergency situations and determines if the event is of a sufficient magnitude to require convening the team. His responsibilities include:

- o Notification of other team members.
- o Ensuring prompt damage assessment.
- o Ensuring safety of team members during completion of duties.
- o Notifying Chief or Assistant Chief, Information Systems Division of status of the **Standard Workstation Cluster** system.

The Chief, Information Center (ADPSO) is also responsible for ensuring computer facility security during assessment procedures, as well as assisting in the surveys of damage to hardware and software components.

1.1.2 System Manager.

The responsibilities of the System Manager in the Disaster Assessment process are to survey and specify physical damage to all electronic components of the **Standard Workstation Cluster** system, and to detail any loss of software as a result of the emergency situation. From this assessment, the System Manager completes the Loss Evaluation Sheets for these items and notifies the Assistant Chief, Information Systems Division of the results.

The System Manager also surveys and reports on damage to terminals, lines, and modems. He also functions as contact to affected users, and reports to the Disaster Assessment Team on communications status.

1.1.3 Chief, Facilities Branch (G-CAS-2).

The Chief, Facilities Branch (G-CAS-2) advises the Disaster Assessment Team of the status of utilities for the **Data Terminal Center**, and coordinates all activities concerning utilities and their interruption/resumption as a result of the emergency. He is responsible for:

- o Electricity.
- o Air conditioning/Ventilation.
- o Telephone.

The Chief, Facilities Branch (G-CAS-2) also advises the Disaster Assessment Team of the status of the physical condition and safety of the **Data Terminal Center**. He determines if the Data Terminal Center meets the physical requirements of **G-TIS** as determined in the contractual agreements or memos of understanding.

**1.2 RESULTS OF DAMAGE ASSESSMENT**

Upon completion of the physical surveys of the **Data Terminal Center**, hardware, and software components, the Disaster Assessment Team will have the information necessary to determine the processing capabilities of **G-TIS** resources.

This information, when compared with the requirement of the applications system as detailed in the Critical Systems Priority List, will be used by the Disaster Assessment Team to decide if operations can be resumed at **G-TIS** or if operations must be moved to an off-site processing location.

The following guidelines are to be followed in making this determination:

- o The **Data Terminal Center** must be physically safe for **G-TIS** personnel to carry out their respective duties.
- o At a minimum, the following hardware, software and supplies must be available to process critical applications
- o Hardware and software needed for critical applications processing is available and functioning.
- o Supplies required are available at the **Data Terminal Center**, or from storage location.

Where these requirements are met, recovery can be accomplished at the **Data Terminal Center** without initiation of backup operations.

Where these requirements are not met, backup operations must be initiated at the off-site location. Restoration of the **Data Terminal Center** will be initiated at the same time.

Encl (2) to COMDTINST M5500.17

**ENCLOSURE 1**

**INFORMATION SYSTEMS DIVISION  
STANDARD WORKSTATION CLUSTER DISASTER ASSESSMENT TEAM MEMBERS**

<b>POSITION TITLE or PERSONNEL DESCRIPTION</b>	<b>NAME</b>	<b>WORK TELEPHONE</b>	<b>HOME TELEPHONE</b>
Chief, Information Systems Division G-TIS	CAPTAIN J.R. Offutt Jr.	(202) 555-5532	
Assistant Chief, Information Systems Division G-TIS-A	J.D. Hargett	(202) 555-5516	
Chief, Information Center (ADPSO) G-TIS-5	LT D. Jones	(202) 555-5581	
System Manager		(202) 555-1234	
Chief, Facilities Branch G-CAS-2	S.H. Wheet	(202) 555-2222	

## ENCLOSURE 2

INFORMATION SYSTEMS DIVISION  
STANDARD WORKSTATION CLUSTER HARDWARE INVENTORY

DESCRIPTION	MODEL NO.	VENDOR	QUANTITY	SIZE/SPEED	COST (OWN/LEASE)	SOURCE
Central Processing Unit	9955	PRIME Computers Inc.	2	5 mb/unit	150,000	PRIME Computer
8 Track Tape Drive	Z27	ACME Mass Storage	12	1600/6250 bpi	60,000	ACME Computer
Video Display Terminals	Q4000	AJAX Television Corp.	8	512k	45 ea/mo.	Reliable Corp.

Encl (2) to COMDTINST M5500.17

**ENCLOSURE 3**

**INFORMATION SYSTEMS DIVISION  
STANDARD WORKSTATION CLUSTER SYSTEM SOFTWARE INVENTORY**

<b>PROGRAM/PACKAGE NAME</b>	<b>RELEASE NO./ VERSION NO.</b>	<b>VENDOR</b>	<b>COST</b>	<b>SOURCE (THOUSANDS)</b>
FORTRAN 66 Compiler	1976	Off-The-Shelf Programs Inc.	200	Compumart Discount Inc.
Source Level Debugger	19.4	ACME Software Products	3.9	K-Mart Department Store

ENCLOSURE 4

INFORMATION SYSTEMS DIVISION  
CRITICAL SYSTEM PRIORITY LIST

APPLICATION NAME	USER REPRESENTATIVE	PROCESSING TIME	DAILY/WEEKLY MONTHLY DEADLINE	ALLOWABLE DELAY
Accounting Balance Tally	George Ledger	2 hours	Bi-weekly	5 days
Monitor Environmental Support	Carl Sagan	4 hours	Bi-monthly	10 days

Encl (2) to COMDTINST M5500.17

**ENCLOSURE 5**

**INFORMATION SYSTEMS DIVISION  
STANDARD WORKSTATION CLUSTER OFF-SITE STORAGE INVENTORY**

<b>DESCRIPTION</b>	<b>SUPPLY/FORM NO. or SIZE</b>	<b>QUANTITY (ON HAND)</b>	<b>COST</b>	<b>SHELF LIFE/ EXPIRATION DATE</b>	<b>SOURCE</b>
Magnetic Tape	8" reels	48	100.00/doz.	NONE	3M Products Inc.
Copy of Facility Contingency Plan	3-ring binder	1	N/A	NONE	AIS Management Staff

ENCLOSURE 6

INFORMATION SYSTEMS DIVISION  
LOSS EVALUATION SHEET

DESCRIPTION	MODEL NO.	VENDOR	QUANTITY	DESCRIPTION OF LOSS or DAMAGE	REPAIR/ REPLACE	ESTIMATED LOSS (HRS.)	UNIT COST
Moving Head Disk Storage	4492	ACME Disk Drives	1	Head crash and fire	REPLACE	300	15,000
Magnetic tape drive units	3399	IBM	8	Heat damage to heads	REPAIR	170	200.00 per unit

Encl (2) to COMDTINST M5500.17

**ENCLOSURE 7**

**INFORMATION SYSTEMS DIVISION  
STANDARD WORKSTATION CLUSTER BACKUP STORAGE INVENTORY**

<b>DESCRIPTION</b>	<b>SUPPLY/FORM NO. or SIZE</b>	<b>QUANTITY (ON HAND)</b>	<b>COST</b>	<b>SHELF LIFE/ EXPIRATION DATE</b>	<b>SOURCE</b>
----- Preprinted forms	GSA 1522a	9 boxes	1,300.00	NONE	Govt. Printing Office

**SAMPLE**  
**BACK-UP PROCESSING**  
**FOR THE**  
**STANDARD WORKSTATION CLUSTER SYSTEM**  
**UNITED STATES COAST GUARD**  
**INFORMATION SYSTEMS DIVISION**

08/10/88

COPY NO. \_\_\_\_\_

**TABLE OF CONTENTS**

<u>SECTION</u>	<u>PAGE</u>
1.0 INTRODUCTION. . . . .	1
1.1 Back-up Team. . . . .	1
1.1.1 Chief, Information Center (ADPSO). . . . .	1
1.1.2 System Manager . . . . .	1
1.1.3 User Representative. . . . .	2
1.1.4 Personnel Movement Officer . . . . .	2
2.0 ENCLOSURE(S)	
Back-up Team Members. . . . .	3

## 1.0 INTRODUCTION

This section describes the actions and procedures needed to accomplish back-up processing for the **Standard Workstation Cluster** system. Back-up processing refers to work activity that cannot be accomplished at the **Data Terminal Center**, and requires implementation of off-site processing. This can result from any of the previously discussed emergency situation.

The Disaster Assessment Team identifies and initiates back-up procedures. The Back-up Team is activated and takes responsibility for movement of media, personnel and data to the off-site locale. These responsibilities are detailed by individual members in the following section. With the loss of availability of the **Data Terminal Center** and the initiation of back-up processing, the next phase in Disaster Recovery is the restoration of the **Data Terminal Center** to a usable state. Restoration activities either at the **Data Terminal Center** or a new site, are implemented concurrent with back-up processing.

### 1.1 Back-up Team.

The Back-Up Team is responsible for the movement of media, data and personnel to the back-up site, the initiation of **Standard Workstation Cluster** processing at the back-up site and the timely completion of these missions. Each individual has assigned duties which are discussed in the following sections. The Backup Team members are listed in Enclosure 4.

#### 1.1.1 Chief, Information Center (ADPSO).

This individual coordinates the activities of the back-up team members, makes decisions on situations that may arise during back-up implementation, and reports progress to the Chief or Assistant Chief, Information Systems Division. The Chief, Information Center (ADPSO) will re-assign team duties as back-up processing progresses in order to support activities involved in the restoration of the **Data Terminal Center**. Additionally, this individual maintains contact with all representatives party to memos of understanding and ensures completion of such agreements.

#### 1.1.1 System Manager.

This individual is responsible for:

- o Ensuring correct hardware configuration is available.
- o Ensuring correct level software is restored.
- o Ensuring priority of critical application processing meets requirements of **G-TIS**.
- o Restoring software to correct levels.

Encl (2) to COMDTINST M5500.17

- o Providing user assistance during processing runs.
- o Correction of program errors.
- o Coordination required to transport back-up tapes from storage location.
- o Coordination required to transport required supplies from storage location.
- o Processing applications in priority sequence.
- o Notification of system and user personnel in case of program error.

1.1.3 User Representative (one per application).

These individuals are responsible for:

- o Input needed to process prioritized critical application.
- o Assistance needed by Programmers and Operators in correcting errors in user programs during processing runs.

1.1.4 Personnel Movement Officer.

This individual is responsible for:

- o Completion of transportation arrangements for personnel to off-site location.
- o Completion of accommodation arrangements for personnel at off-site location.

**ENCLOSURE 1****INFORMATION SYSTEMS DIVISION  
STANDARD WORKSTATION CLUSTER BACKUP TEAM MEMBERS**

<b>POSITION TITLE or PERSONNEL DESCRIPTION</b>	<b>NAME</b>	<b>WORK TELEPHONE</b>	<b>HOME TELEPHONE</b>
Chief, Information Systems Division G-TIS	CAPTAIN J.R. Offutt Jr.	(202) 555-5542	
Assistant Chief, Information Systems Division G-TIS-A	J.D. Hargett	(202) 555-5595	
Chief, Information Center (ADPSO) System Manager	LT D. Jones	(202) 555-5520 (202) 555-1234	
User Representative (One Per Application)		(202) 555-6541	
Personnel Movement Officer		(202) 555-8888	

Encl (2) to COMDTINST M5500.17

**SAMPLE**  
**DISASTER RECOVERY**  
**FOR THE**  
**STANDARD WORKSTATION CLUSTER SYSTEM**  
**UNITED STATES COAST GUARD**  
**INFORMATION SYSTEMS DIVISION**

08/10/88

COPY NO \_\_\_\_\_

**TABLE OF CONTENTS**

<u>SECTION</u>	<u>PAGE</u>
1.0 INTRODUCTION. . . . .	1
1.1 Responsibilities of Disaster Recovery Team. . . . .	1
1.1.1 Chief, Information Center (ADPSO). . . . .	1
1.1.2 System Manager . . . . .	2
1.1.3 Chief, Facilities Branch (G-CAS-2) . . . . .	2
1.2 Recovery Actions. . . . .	2
2.0 ENCLOSURE(S)	
Recovery Team Members . . . . .	3

## 1.0 INTRODUCTION

This section of the contingency plan describes the actions and processes necessary to return the **Standard Workstation Cluster** system to full operational status as a result of system degradation (partial loss of operating capability) or a total system loss/failure.

With the determination by the Disaster Assessment Team that recovery is possible at the **Data Terminal Center** (i.e. off-site operations not required), the goal is to achieve system recovery in a timely and cost-effective manner while minimizing adverse impacts on the mission and users of the **Standard Workstation Cluster** computer facility.

The strategy to meet this goal involves implementation of a three-stage plan:

- o Stage I. Use available facility/equipment to process prioritized critical applications.
- o Stage II. Replacement/repair of system components and facilities damaged as a result of the emergency to provide on-site processing of critical production applications.
- o Stage III. Replacement/repair of system components and facilities to allow for new development processing - essentially a return to pre-disaster status.

### 1.1 Responsibilities of Disaster Recovery Team.

The Recovery Team is responsible for the implementation of the recovery plans and processes to ensure the timely restoration of each level of operation. Each individual has assigned duties to accomplish within each step of recovery actions.

The following section details the individual responsibilities for the members of the Recovery Team. The Recovery Team members are listed in Enclosure 1.

#### 1.1.1 Chief, Information Center (ADPSO).

This individual coordinates the activities of the recovery team members, makes decisions when any conflicts arise during the recovery process, and reports progress to the Chief or Assistant Chief, Information Systems Division. This individual also coordinates recovery requirements and progress with the Chief, Facilities Branch (G-CAS-2) when repair to the **Data Terminal Center** or utilities is necessary. In addition, this individual enforces memos of understanding wherever applicable. He oversees replacement/purchasing of new hardware and software

as required. He makes the final recommendation as to when to return data processing functions to the **Data Terminal Center**. This individual is also responsible for:  
ADP security during recovery process.  
ADP security of new site if applicable.  
Coordinating recovery activities with remote users requirements and the System Manager.

#### 1.1.2 System Manager.

This individual is responsible for determining any reconfiguration of the system hardware that is necessary to meet the goals of the recovery process. He is also responsible for:

- o Ensuring correct level of software is available to users.
- o Ensuring correct hardware is available.
- o Ensuring priority of applications processing meets requirements of **G-TIS**.
- o Restoring software to level prior to the emergency.
- o Providing assistance to users during processing runs.
- o Correcting program errors caused by changes to system availability due to emergency situations.
- o Obtaining any required system and application backup tapes from storage locations.
- o Obtaining any required supplies from storage locations.
- o Processing applications in priority situations.
- o Notification of system or user personnel in case of program errors.

If restoration of the facility is required this individual is responsible for verifying completion of electronic equipment installation.

#### 1.1.3 Chief, Facilities Branch (G-CAS-2).

The Chief, Facilities Branch (G-CAS-2) is responsible for the completion of facility and utilities for the **Standard Workstation Cluster** system requirements. Those requirements are detailed in the memos of understanding (Enclosure 2) for the **Data Terminal Center**.

### 1.2 Recovery Actions.

The first recovery action is to use any available equipment to process the prioritized critical applications. This is accomplished by providing the minimum hardware requirements needed by the critical applications and the latest backup version of the software available. The hardware availability determines how many applications can be processed at any one time. If damage is too severe, back-up (off-site) operations will be initiated and the Recovery Team will implement Stage II recovery.

The Operations Instructions detail step-by-step instructions to be followed by operations for such events as:

- o System halts.
- o Directory restorations.
- o File restoration.
- o System dumps.
- o Disk backup.

These instructions are accompanied by operations instructions for each critical application. Both of these guides are used in conjunction with procedures developed to deal with event related contingencies such as:

- o Loss of a disk pack.
- o Loss of string of disk devices.
- o Loss of tape drives.
- o Loss of printers.
- o Loss of terminals (local and remote).
- o Loss of combination of the above.

Encl (2) to COMDTINST M5500.17

**ENCLOSURE 1**

**INFORMATION SYSTEMS DIVISION  
STANDARD WORKSTATION CLUSTER RECOVERY TEAM MEMBERS**

<b>POSITION TITLE or PERSONNEL DESCRIPTION</b>	<b>NAME</b>	<b>WORK TELEPHONE</b>	<b>HOME TELEPHONE</b>
Chief, Information System Division G-TIS	CAPTAIN J.R. Offutt Jr.	(202) 555-5534	
Assistant Chief, Information Systems Division G-TIS-A	J.D. Hargett	(202) 555-5523	
Chief, Information Center (ADPSO) G-TIS-5	LT D. Jones	(202) 555-5533	
System Manager (202) 555-1234			
Chief, Facilities Branch G-CAS-2	S.H. Wheet	(202) 555-2222	

SAMPLE

915 Second Avenue  
Seattle, WA 9  
8174-1067  
Staff Symbol:  
(dt)  
Phone:  
FTS 399-5830  
AVN 941-3441  
5500

From: Commander, Thirteenth Coast Guard District

To : Commander, Coast Guard Group North Bend

Subj: ACCREDITATION OF GROUP NORTH BEND PERSRU STANDARD  
WORKSTATION CLUSTERS

Ref : (a) COMDTINST M5500.13 (series), AIS Security Manual

1. I have reviewed the Automated Information Systems (AIS) Security Plan, Contingency Plan, and Risk Assessment Report for the Group North Bend PERSRU Standard Workstation Cluster system. I found this system is operating at an acceptable level of risk for processing sensitive but unclassified information in accordance with reference (a).

2. I authorize operation of the Information System Division Standard Workstation Cluster system to process sensitive but unclassified information. This system shall be re-accredited as required by reference (a).

I. M. INCHARGE

By direction

SAMPLE

**EXAMPLES OF CUSTOMIZED USER COMMAND SETS**

Users should be limited to those Standard Workstation commands they need to do their job and have the skills to use (See chapter 3 paragraph 5 of this handbook). This will help control access to files by reducing the risk caused by untrained users. Below are three examples of command sets which might be used by three different levels of users.

Example of ClassA.cmds List: (System Managers should have all available commands if they so desire.)

Append	MCluster Status
Assemble	MCopy
Bootstrap	MCreate Configuration File
Clean Up	MCreate Directory
Cluster Status	MDelete
Command File Editor	
Create file	MDisable Cluster
Debug File	MFiles
Delete	MISAM Configure
Dump	MISAM Copy
Edit	MISAM Delete
Files	MISAM Install
Forms Editor	MISAM Rename
Install Queue Manager	Misam Reorganize
Install Spooler	MISAM Set Protection
IVolume	MISAM Status
LCopy	MISAM Terminate
Librarian	MIVolume
Link	MMerge
Logout	MPartition Status
MBackup Volume	MPlog
MChange Volume Name	MRemove Directory
MCLI	MRemove Directory
MRename	New Command
MRestore	Path
MResume Cluster	Print
MSelective Backup	Record
MSet Directory Protection	Remove Command
MSet Protection	Replay
MSort	Run
MSpooler Status	Screen Setup
MTape Backup Volume	Set Time
MTape Copy	Stop Record
MTape Initialize	Submit
MTape Restore	Type
MTape Selective Backup	User File Editor
MVolReport	Volume Status
MVolume Status	

Encl (4) to COMDTINST M5500.17

Example of ClassB.cmds list: (for experienced users with local file systems, or programmer)

ADS	Driver
Append	Edit
Assemble	Files
Backup Volume	Floppy Copy
Basic	Format
Clean	Forms Editor
CM Add Application	FORTRAN
CM Config File Editor	
CM Modify Info	Install Context Manager
CM Remove Application	Install Mail Server
Cobol	Install Remote Mail Manager
Configure Mail Center	Install Spooler
Copy	ISAM Configure
Corporate Agenda	ISAM Copy
Create Configuration File	ISAM Create
Create File	ISAM Delete
CRun	ISAM Install
Debug File	ISAM Rename
Deinstall Mail Server	ISAM Reorganize
Deinstall Mail Server	ISAM Set Protection
Deinstall Remove Mail Manager	ISAM Status
ISAM Terminate	Print
IVolume	Reassociate ISAM
LCopy	Record
Librarian	Recover
Link	
LInstall	Rename
List	Replay
Logout	ReQuest
Mail	Restore
Maintain File	Resume Mail Server
Make Wheel Set	Run
Merge	Run File
Mplog	Screen Setup
MSDOS	Selective Backup
MSDOS Create Pseduo-volume	Set Corp Password
MSDOS Read	Set File Prefix
MSDOS Write	Sort
Multiplan	Spooler Status
	Stop Record
Path	Submit
Picture Editor	Suspend Mail Server
PLog	Task Master
Task Utility	Volume Status
Type	Word Processor

Example of ClassC.cmds list: (for users with limited experience or limited needs to do their job)

ADS	Print
Asynchronous Terminal Emulator	Remove Command
Copy	Remove Directory
Create Directory	Rename
Edit	Restore
Files	ReQuest
File Manager	Screen Setup
IVolume	Selective Backup
Logout	Spooler Status
Mail	Submit
Multiplan	Type
Path	Volume Status
Picture Editor	Word Processor