Forest Service Handbook
National Headquarters - Washington Office
Washington, DC

Forest Service Handbook 6609.12 – ADP Technical Approval Handbook
Chapter 20 – System Resources Management

Amendment: 6609.12-1991-1

Effective date: September 03, 1991

Duration: This amendment is effective until superseded or removed.

Approved by: F. Dale Robertson, Chief

Date approved:

Responsible Staff:

Last Change:

Superseded Document(s): Entire Handbook issued August 1986; Title Page; 00—1 thru 23

Digest: Following is an explanation of the changes throughout the directive by section.

This amendment is a reissuance of FSH 6609.12 to conform the format and structure of the Handbook to the requirements of electronic directive issuance.

This amendment makes no substantive changes to the text. The only changes made are those necessary to meet new format requirements or to correct spelling, punctuation, or unit names.

This Handbook is now available electronically in the National Information Center in the same format as the paper copy. Henceforth, amendments to this Handbook will be issued to Forest Service units electronically on a document basis.

Table of Contents

21 - Physical Security and Protection

As a natural consequence of the increase in computer capacity within the Forest Service, more and more office paperwork processes are being converted to the Data General systems. This results in a need for better system security and hardware protection to reduce or prevent unauthorized access, damage or loss. See chapter 10 for access management security issues.

21.1 - Physical Security

Protection of the equipment is as important as managing system or file access. Hardware that is vital to system operations, such as the CPU, disks, tape drives, and master console must be secure from uncontrolled access. This equipment and associated devices shall be kept in a computer room that is not readily accessible to the general user community without supervision by system management personnel. The master console shall be put into LOCK_CLI mode when not attended, and must not be made available for use by non-systems personnel at any time. During non-business hours, the computer room shall be locked to prevent unauthorized entry.

21.2 - System Maintenance

Two types of work need to be performed on the Data General equipment, hardware repair and preventive maintenance. Both are important in reducing system downtime.

The CPU and the master console must be on either the full or cooperative maintenance program with Data General. The master console is not considered to be a peripheral console, whether it is used as such or not. Hardware repair for peripheral devices comes in four options: full or cooperative maintenance; a mail-in option; and self-repair of the equipment. Full and cooperative maintenance options are Data General programs, the first involving repair by Data General personnel and the second involving repair by trained Forest Service or Data General employees, depending on the nature of the problem. With these options, repair parts are owned by Data General. Mail-in options are available from Data General or third-party vendors, and basically involve sending parts to a central location for repair or replacement. Depending on the contract specifications for this type of program, parts may be owned by the vendor or purchased by the Forest Service. Self-repair consists of buying parts from vendors and repairing the equipment on-site. The actual and potential expenses of each of these options vary with the type of coverage. A close examination of each should be made so that line managers can make an informed decision on which type of program to implement.

The potential for damage to the system is greatly reduced through implementation of a preventive maintenance program. Preventive maintenance measures shall be undertaken only by authorized personnel who have been trained in the proper procedures. The authorized and qualified personnel are determined in part by the type of hardware repair program a site is using. Sites with full maintenance will have preventive maintenance performed on the enrolled equipment by the Data General field engineer. Sites under cooperative maintenance shall have

the preventive maintenance performed by or under the supervision, of Forest Service employee(s) trained in that area. Under no circumstances shall maintenance be performed by anyone other than trained individuals.

21.3 - System Protection

Measures must be taken to protect the system from damage by outside forces such as power fluctuations, lightning, fire, water and earthquake damage, and temperature and humidity extremes. Information on basic environmental standards can be found in the "How To Generate And Run AOS/VS" manual or the site preparation guidelines.

Lightning and an inconsistent power supply are two problems that can easily cause repeated damage to a system if they are not addressed. Although lightning can cause major damage to a system and is hard to predict or control entirely, there are some things that can be done to reduce its potential effects. When lightning activity in the area is determined to be potentially harmful to the system, the system should be shut down and unplugged. All peripherals should also be unplugged from their power source, and if non-grounded data cables run from one building to another, they should be unplugged at both ends to prevent lightning from traveling up those lines and damaging equipment. In areas where power fluctuations create problems, it is recommended that an analysis be performed to determine the justification for installing a power conditioner (or similar device) between the incoming power and the CPU. Other devices such as surge protectors may be used to protect peripherals. Port protectors can be used to furnish some protection to the IACs.

The likelihood of fire and water damage occurring is less than having power problems, but there are steps that can be taken to reduce the risk and effect. Halon fire extinguishers shall be located within the computer room and personnel should be trained in their use. Where feasible, a raised floor should be installed to help protect against water damage. Backup media shall be stored in fireproof enclosures where available, and at least one set of backup tapes shall be stored at a remote disaster site.

In some areas, earthquakes and similar natural disasters pose a threat and measures should be taken to minimize potential damage. Besides damage resulting from falling objects, dust, or sudden movement of the equipment, fire is a very real danger in these situations, and proper precautions as stated above should be taken.

It is important to note that these problems are excluded under the Data General maintenance contract and third-party contracts, and can be very costly to recover from. In many instances, advanced preparation can minimize or eliminate these additional expenses.

21.4 - Disaster Plan

Each Forest Service installation with Data General equipment shall have a risk assessment, a security plan, and a disaster storage site for backup tapes that is removed from the facility in

which the system is located. Weekly backup tapes shall be rotated to and from the disaster storage site to the main facility on a regularly scheduled basis to provide maximum protection of files. An extra copy of the latest revisions of the SYSTAPE and Products Tapes shall also be stored. Storage of the tapes at the remote site should meet conventional standards and access to the tapes should be restricted to authorized personnel only. In addition, the facility used as a disaster storage site shall meet the required environmental standards for tape storage.

22 - Monitoring System Performance

22.1 - System Performance and Resource Demands

Monitoring system performance is difficult at best as there are no strict, quantitative guidelines. Monitoring is useful for three reasons: to establish workload trends and determine when additional hardware capacity is needed; to gather baseline data for developing advice to the local line officer in making decisions regarding the best utilization of existing equipment; and to determine if any damaged or runaway processes are usurping system resources.

22.11 - Data Collection

Several standard software packages are provided that will enable the System Manager to collect data that describe or yield indicators of overall system performance. These are: TIMER, VMON, DISCO, and PED. Several of these systems are accessed through "Utilities" activities on the "FS System Manager Functions" menu.

22.11a – TIMER

This system uses a special profile (see section 11.2) to perform repetitive CEO tasks. The start/stop time is automatically recorded and summary reports can be generated. Data should be collected while the system is operating normally with all standard servers running and/or users logged on. To run TIMER, select "Response Time Information" from the "FS System Performance Utilities" menu. The quality and reliability of the data gathered will depend upon the number of runs and times selected to perform a TIMER run. It is recommended that TIMER be run at least four times per day over a three day period to establish a valid record of CEO response time. Trends can be documented by comparing TIMER reports periodically. The summary reports can be generated through the "Response Time Information" activity under the "FS System Performance Utilities" menu.

22.11b – VMON

This program will display data that describes the general workload and demands being placed upon AOS/VS to process system and user requests. To run VMON, select "AOS/VS Information" from the "FS System Performance Utilities" menu. The screen can be updated so that current data will be displayed. VMON displays data on PID activity, CPU utilization, Cache Buffer hit ratio, and memory utilization. The file VMON.DOC in :PUBLIC:DOCUMENTATION:IS provides

detailed information on the use and interpretation of VMON. The "How to Generate and Run AOS/VS" manual contains more information on memory management and general system performance topics.

22.11c – DISCO

The DISCO program provides data on the workload and demands placed on each disk on the system. The data on "% Busy" and "% Total" can be used in making decisions about the placement of user directories and the best way to balance the overall I/O load on the system. The data on "Max/Average Queue length" can help determine if an I/O processing bottleneck is affecting system response time. The data on "Seek" can be used to reveal disk fragmentation and to determine if it would be wise to reformat disks (refer to the "How to Generate and Run AOS/VS" manual). DISCO is run by selecting "Disk Information" from the "FS System Performance Utilities" menu.

22.11d – PED

Process Environment Display (PED) can be used to reveal the operating behavior of an individual process on the system. It will display data that describes the memory and I/O demands placed upon the system by a process. These data are useful in investigating new software or program changes. Once data have been established for a process, they need not be collected again unless the program changes. The "How to Generate and Run AOS/VS System" manual contains complete instructions on running PED.

22.12 - Space Reports

A report on space usage can be run by selecting "Space Utilization" from the "System Manager's Reports" menu. This report should be run periodically depending upon the activity at a particular site. The data collected will provide a history of the growth and management of the system's storage resources.

22.2 - Examination and Storage of System Logs (SYSLOG)

AOS/VS system activities must be logged in SYSLOG files on all FS systems at all times. The UP macro will ask whether to create a new SYSLOG file and will rename and move old files to a storage directory if this option is selected.

22.21 – Examination

The "How to Generate and Run AOS/VS" manual contains detailed information on the types of reports that can be generated from the SYSLOG files. The most important data stored in SYSLOG is information about access to the system. A review of access to the system by guest, non-local, privileged and functional profiles, and information on retrievals and DCC activity, can be compiled by running the FSIA_SCAN macro. The system manager is responsible for

establishing a regular timetable (for example, monthly or bi-weekly) by which the SYSLOGs created during the period are to be examined using the FSIA_SCAN procedure to determine if any improper access or activity has occurred.

22.22 – Storage

To conserve disk space, these files must be periodically placed on tape and safely stored in the local tape library. SYSLOG files must be kept for a minimum of five years (Statute of Limitations; U.S. Code, Title 18, Section 3282).

22.3 - Use of Consumable Supplies

As part of managing the operation of a computer system, the System Manager should monitor the use and stocking levels of expendable supplies such as paper, ribbons, thimbles, etc. Excessive use of these items can indicate a potential hardware or software problem or a need for better user education (see also Section 27 - Supply Management).

23 - System Utilization

It is a System Management function to provide advice, guidance, and fully developed alternatives for decisions by line management in the use, support, and operation of the local DG system. Each site should determine how to best support this function.

23.1 - Analyzing System Use Trends

By using data collected by the methods described in section 22, the System Manager can evaluate trends in system use. Trends should be evaluated with respect to the overall workload to determine if periods of heavy system use are from a situational deadline or impact, or from steady, gradually increasing use of the system.

23.2 – Mitigation

There are some specific steps that the System Manager can implement to mitigate an overloaded system. Throughout the day, system use will generally have well-defined peaks. Employees should be encouraged to use the system more heavily during non-peak times. Many reports can be run in batch after normal working hours. Large data files can be transmitted or retrieved at night, which will not only reduce demands on the disk(s) but will also lower communications costs overall (see section 14.4). All systems do not need every DG product; refer to the 6620 manual for a list of the mandatory software. The System Manager should ensure that the cache buffer size is correct (see section 31.4). Data from VMON can be used to determine if the system is memory-bound or compute-bound. On systems with more than one disk, DISCO data should be examined to check the workload distribution over all disks (see section 22.1).

24 – Backups

To ensure minimal system downtime and reduce loss of data, systems shall be backed up on a regular basis. Four sets of backup media must be maintained: the SYSTAPE; the Products Tapes; the FULLDUMP tapes; and the CHANGETAPE tapes.

Current backups help recover files in the event of a crash or file deletion. Downtime is reduced when proper recovery techniques are used.

24.1 - The SYSTAPE

Create a new SYSTAPE after every update to the installed system or the system directories associated with it. The SYSTAPE contains all of the software necessary to bring the system up from SCP-CLI to the AOS/VS prompt. Immediately after a new SYSTAPE is created, test it out by trying to boot the system from it. This tape is used to reload the system in the event of a crash in which system software is damaged or destroyed. Two copies of this tape are required: the first should be stored in the vicinity of the computer, and the second shall be stored at the disaster site.

24.2 - Products Tapes

These are a set of tapes that contain software that is not essential in bringing the system up. They will contain products used to create the working environment for users, such as FSIA and the CEO products. Also included are programming language directories, utilities documentation, macro libraries, network and graphics software, and other products. To keep this system standard throughout the Forest Service, only the products referred to in the SYSTAPE_PROD.CLI macro should be dumped to these tapes. Other directories and macros that a unit may want to back up should be handled by the FULLDUMP and/or CHANGETAPE. A copy of these tapes shall be sent to the disaster site for use in emergency situations.

24.3 - Weekly Full Backups

Once a week, the system shall be backed up to tape. It is not necessary, or even recommended, to dump everything from disk. At a minimum, all directories and files that are considered necessary or desirable, and which are not available on the products tapes or the SYSTAPE, must be backed up. Information of a non-essential or temporary nature may not need to be backed up, depending on local policy. It is important to remember that files that are not backed up cannot be recovered if they are deleted from the system or otherwise corrupted.

It is strongly recommended that IVERIFY be run on the CEO_INDEX prior to running a FULLDUMP to be sure that the index is correct. Backing up a corrupted database is useless, and can result in serious problems.

Depending on the needs and desires of the local user community, three or more sets of backup tapes should be maintained. At least one set shall be kept at the disaster site (see 21.4).

24.4 - Daily Incremental Dumps

Every working day, a backup of the files that have been changed or added to the system shall be done. The process can dump all of the files changed or added since the last FULLDUMP, or since the last daily backup was performed. It is a local decision as to which of these methods is implemented.

To minimize the impact on the user community, it is recommended that this be done in batch at night, using the CHANGETAPE routine. See the information on this in :FS:CHANGE.TAPE.MACROS.

24.5 - File Recovery

In the event of corruption or deletion of files, it may be necessary to use some procedure to recover those files. Files can be recovered from the daily backup tapes and the products tapes by using the LOAD or LOAD_II utilities. Recovery from labeled multiple-tape sets such as the FULLDUMP is more complicated. Refer to the "How To Generate and Run AOS/VS" manual.

24.6 - CEO Archiving

Where the use of CEO archiving has been approved by management, encourage the utilization of this feature for only those documents that will not be required for a long period of time. Discourage the use of this option to temporarily reduce disk space. When used as a mechanism to temporarily reduce disk space, ineffective utilization of system operator and magnetic tape resources will result.

25 - System Updates

The Washington Office CS&T, Software Management Group is responsible for the creation and distribution of service-wide software updates. Refer to FSM 6620. The System Manager is responsible for the installation and implementation of each update by the required dates.

25.1 - Mandatory Software

All sites must install and maintain common system software to gain maximum benefits from sharing software and support services, and to implement Service-wide information management processes. These software packages must be installed on all Forest Service Data General systems. Mandatory software may change as more advanced software technologies evolve and are incorporated into Service-wide information processing technology.

25.11 - Data General System Software

See section 28, exhibit 01.

25.12 - Forest Service System Software

See section 28, exhibit 01.

25.13 - Forest Service Functional Software

Some functional (staff) software, such as the "Time and Attendance" system, will be mandatory for all sites. Refer to FSM 6620 for a description of the responsibilities and the approval process for functional systems. Refer to section 51 for a discussion of the coordination between the System Manager and Staff Information Manager needed to install and implement mandatory functional software systems.

25.2 - Optional Software

The System Manager plays an important role in the evaluation of optional software systems and their ability to satisfy local information management needs. In this capacity, the System Manager provides advice and guidance to the local line officer who will make decisions regarding the implementation and use of optional software packages. Refer to FSM 6620. Technical characteristics of the software, such as space used and file access method are only two aspects to be considered and balanced with the advantages the software offers in supporting information management for the unit. The System Manager shall keep accurate records of all optional software approved for local use.

26 - System Cleanup

26.1 - System Management Related Files

A cleanup macro is included with each system update. The System Manager should ensure that this is run after each update is correctly installed. Additionally, obsolete macros and directories should be removed from the system regularly.

26.2 - User Liaison

As part of the coordination responsibilities, the System Manager shall work closely with the Staff and Public Information Managers to assist them with managing their cabinets, identifying obsolete files, and providing advice on how to best manage their available space.

27 - Supply Management

The System Manager should coordinate with those responsible for ordering computer-related supplies to make sure that appropriate stocking levels are maintained. These coordination efforts should include provisions for proper handling and storage of supplies. To provide input to supply ordering decisions, consider developing a regular inventory system to establish normal consumption levels.