



U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
Air Traffic Organization Policy

ORDER
JO 6130.3A

Effective Date:
5/7/09

SUBJ: Maintenance of Flight Data Input/Output (FDIO) Equipment

1. PURPOSE.

This handbook provides guidance and prescribes technical standards, tolerances, and procedures applicable to the maintenance and inspection of Flight Data Input/Output (FDIO) equipment. It also provides information on special methods and techniques which will enable maintenance personnel to achieve optimum performance from the equipment. This information augments information available in instruction books and other handbooks, and complements the latest edition of Order 6000.15, General Maintenance Handbook for National Airspace System (NAS) Facilities.

2. DISTRIBUTION.

This order is distributed to selected offices and services within Washington headquarters, Technical Operations Services (TOS), Service Area Offices, Engineering Services Offices, Technical Services Offices, Mission Support Offices, William J. Hughes Technical Center (WJHTC), Mike Monroney Aeronautical Center, TOS field offices responsible for the maintenance of FDIO equipment.

3. CANCELLATION.

This Order cancels Order JO 6130.3, Maintenance of the Flight Data Input/Output (FDIO) Equipment, dated June 1, 2006.

4. EXPLANATION OF CHANGES.

Configuration Control Decision (CCD) N31357, Hardware Change for the ECG FDIO/CCU Sustainment Project, authorizes the replacement of the FDIO Central Control Unit (CCU) at Air Route Traffic Control Centers (ARTCC) with the FDIO-Gateway (FDIO-G).

5. MAINTENANCE AND MODIFICATION PROCEDURE.

a. The Order 6000.15, this handbook, the applicable equipment instruction books, and other applicable handbooks shall be consulted and used together by the maintenance technician in all duties and activities for the maintenance of FDIO equipment. These documents shall be considered collectively as the single official source of maintenance policy and direction authorized by the Air Traffic Organization (ATO). References located in the appropriate paragraphs of this handbook entitled: Chapter 3, Standards and Tolerances; Chapter 4, Periodic Maintenance; and Chapter 5, Maintenance Procedures, shall indicate to the user whether this handbook and/or the equipment instruction book shall be consulted for a particular standard, key inspection element or performance parameter, performance check, maintenance task, or maintenance procedure.

b. The latest edition of Order 6032.1, National Airspace System Modification Program, contains comprehensive direction concerning the development, authorization, implementation, and recording of modifications to facilities, systems, and equipment in commissioned status. It supersedes all instructions published in earlier editions of maintenance technical handbooks and related directives.

c. Modifications to equipment that is baselined under configuration management shall be in accordance with the latest edition of Order 1800.66, Configuration Management Policy.

6. RECOMMENDATIONS FOR IMPROVEMENT.

This handbook is under configuration management control as defined in Order 1800.66, and NAS-MD-001, NAS Configuration Management Document. Any changes to the baseline document or requests for deviation from national standards shall be processed through the NAS Change Proposal (NCP) process. Copies of the NAS Change Proposal Form (FAA 1800-2), are provided in the back of this handbook for the convenience of handbook users.



Henry Gonzalez
Director, Program Operations

TABLE OF CONTENTS

<i>Paragraph</i>	<i>Page</i>
Chapter 1. GENERAL INFORMATION AND REQUIREMENTS	
100. Objective	1
101. Coordination	1
102. Periodic Maintenance	1
103. Interruptions Reporting	1
104. Standardization	1
105. References	1
106.–199. Reserved	1
Chapter 2. TECHNICAL CHARACTERISTICS	
200. General	3
201. CCU	4
202. FDIO–G	4
203. RCUs	6
204. PC–RCU	7
205. RFSP	8
206. RANK	8
207. CRT	8
208. FDIO Peripheral Emulation	8
209. FDIO External Connections	9
210.–299. Reserved	9
Chapter 3. STANDARDS AND TOLERANCES	
300. General	15
301. FDIO Equipment	16
302. CCU	17
303. FDIO–G	17
304. RCU	18
305. PC–RCU	18
306.–399. Reserved	18
Chapter 4. PERIODIC MAINTENANCE	
400. General	19
Section 1. PERFORMANCE CHECKS	
401. FDIO	20
402. FDIO–G	21
403. PC–RCU	21
404.–449. Reserved	21

TABLE OF CONTENTS (Continued)

Paragraph *Page*

Section 2. OTHER MAINTENANCE CHECKS

450.	FDIO Equipment	22
451.–499.	Reserved	24

Chapter 5. MAINTENANCE PROCEDURES

500.	General	25
------	---------------	----

Section 1. PERFORMANCE CHECK PROCEDURES

501.	General Performance Check Procedures	26
502.	TD Procedure for the En Route Center, Terminal, or OFDPS Facility ...	26
503.	TD Procedure for FDIO Printers and CRTS at the OFDPS Facility.	26
504.	TD Procedure for the Alaska Center to Terminal Facility.	27
505.–539.	Reserved.	27

Section 2. OTHER MAINTENANCE TASKS

540.	General Maintenance Tasks	27
541.–569.	Reserved	27

Section 3. SPECIAL MAINTENANCE PROCEDURES

570.–599.	Reserved	27
-----------	----------------	----

Appendix 1. CERTIFICATION REQUIREMENTS

Appendix 2. GLOSSARY OF TERMS AND ABBREVIATIONS

Appendix 3. ABBREVIATIONS

Appendix 4. SENSITIVE SECURITY INFORMATION AND MAGNETIC MEDIA DISPOSAL/REUTILIZATION POLICY/PROCEDURES

Appendix 5. POLICY/PROCEDURES FOR IDENTIFYING, HANDLING, MARKING AND DIS- POSAL OF SENSITIVE UNCLASSIFIED INFORMATION (SUI)

LIST OF ILLUSTRATIONS

<i>Figure</i>	<i>Page</i>
2-1. ARTCC FDIO System Functional Block Diagram	10
2-2. FDIO-G System Functional Block Diagram	11
2-3. OFDPS (HCF) FDIO System Functional Block Diagram	12
2-4. Alaska FDIO System Functional Block Diagram	13
2-5. Terminal/Offshore FDIO System Functional Block Diagram	14

CHAPTER 1. GENERAL INFORMATION AND REQUIREMENTS

100. OBJECTIVE.

This handbook provides the necessary guidance, to be used in conjunction with information available in instruction books and other handbooks, for the proper maintenance of Flight Data Input/Output (FDIO) equipment.

101. COORDINATION.

a. Any maintenance activity on the FDIO remote equipment shall be closely coordinated at all times with Air Traffic (AT) operations, the servicing Air Route Traffic Control Center (ARTCC) National Air Space (NAS) Operations Manager (NOM), and any required military operations personnel to preclude unanticipated interruption of service.

b. Technicians assigned to the facility where FDIO equipment has been installed shall be responsible for maintaining the equipment in an operational condition within the tolerance specified in chapter 3 of this handbook.

c. Cognizant AT operations personnel shall be advised immediately of equipment failure, restoration to service, and whenever the established tolerances are exceeded or are expected to be exceeded. This is especially important where standby or spare equipment is not immediately available. In any case in which equipment operation may be adversely affected, sufficient advance notice shall be given to AT operations personnel, since Air Traffic Control (ATC) procedures are based on the assumption that all equipment is available.

d. It is also expected that AT personnel will recognize the need for releasing equipment at the scheduled time for routine maintenance tasks and will offer cooperation in the furtherance of practices that assure continuous and reliable operation.

102. PERIODIC MAINTENANCE.

Maintenance personnel shall follow the tasks and schedules provided in chapter 4, which include the minimum essential preventive maintenance activities and the frequency with which they shall be performed so as to meet the minimum performance standards for the FDIO equipment.

103. INTERRUPTIONS REPORTING.

Interruptions to FDIO equipment shall be reported in accordance with the latest edition of Order 6040.15, National Airspace Performance Reporting System (NAPRS).

104. STANDARDIZATION.

Agency policy provides that all FDIO equipment used for a specific purpose be standardized both electrically and mechanically. The inclusion of any equipment item in this handbook is not justification for field procurement of such items without prior coordination with, and approval by, the Systems Maintenance Service.

105. REFERENCES.

a. The nature of this document requires reference to numerous publications. To avoid frequent revision for the purpose of changing references to the latest issue, personnel shall consider all references to refer to the most recent edition.

b. A list of related publications useful to technical personnel may be found in Order 6000.15, appendix 1.

c. A listing of documents useful to NAS personnel may be found in the catalog of documentation maintained by the National Airspace System Documentation Facility.

106.–199. RESERVED.

CHAPTER 2. TECHNICAL CHARACTERISTICS

200. GENERAL.

a. The FDIO equipment is used in the following environments: En Route Centers, Terminal, Offshore, and Center Radar Approach Control (CERAP).

(1) In the En Route environment the FDIO Central Control Unit (CCU) interfaces with the FDIO Remote Control Unit (RCU) or the Personal Computer-Remote Control Unit (PC-RCU) at the tower, Tower Radar Approach Control (TRACON), and military facilities. FDIO-G replaces the CCU at selected ARTCCs and interfaces with PC-RCU, only. The Alaska center's flight data processor communicates directly with the associated tower peripherals.

(2) In the Terminal environment (tower, TRACON, and military) facilities the FDIO RCU or PC-RCU interfaces with the centers CCU or off shore Honolulu Control Facility (HCF) series-1 equipment. The PC-RCU will also interface with the center's FDIO-G. RCU or PC-RCU drives local FDIO printers, monitors, keyboards, and external interfaces. In the Alaska environment, the tower's PC-RCU communicates with the center's Flight Data Processor (FDP).

(3) In the Offshore environment (Offshore Flight Data Processing System (OFDPS)) the OFDPS Series-1 Replacement (S1R) interfaces with the local PC-RCUs and terminal PC-RCUs. FDIO printers are used, but the keyboards for FDIO are a function of the OFDPS system. The FDIO system supplies an interface box between the PC-RCU and the local Video Graphic Array (VGA) monitors.

(4) In the San Juan CERAP environment, the local PC-RCUs are driven via the Miami center FDIO-G (local HOST patch in Miami allows CERAP to accept strips as En Route and accepts controller messages to Miami as En Route). The PC-RCUs drive local FDIO printers using En-Route formatted strips, monitors, and keyboards.

b. The following FDIO equipment is used in the different environments:

(1) En Route Centers:

CCU or

FDIO-G

Peripherals: none

(2) Terminal (FAA and military):

RCU or

PC-RCU

Peripherals: keyboard, monitor, printer

(3) Offshore (HCF):

PC-RCU

Peripherals: printer

Interface box (between VGA monitor and PC-RCU)

(4) CERAP (San Juan):

PC-RCU

Peripherals: keyboard, monitor, printer

c. The FDIO system receives flight plan data, weather information, and general information from the central computer system at the ARTCC, the OFDPS located in Hawaii and the FDP located in Alaska. The FDIO system also distributes flight plan data to the center and offshore systems, where it is sent on to the central computer for processing. The central computer then sends the information to ATC users as required. Refer to figures 2-1 through 2-5, (FDIO system functional block diagrams) for the center, terminal, offshore, and Alaska overview.

201. CCU.**a. GENERAL.**

(1) The CCUs are located at the ARTCC. Each CCU controls and routes data to and from a maximum of 28 remote sites via modems, using RS-232C interface.

(2) One or two CCUs can be mounted in a single cabinet.

(3) Each CCU consists of 19-inch rack mounted electronic chassis: ten power supplies, two multi-bus processors, and the number of bus connector assemblies required for that facility.

(4) Each CCU is made up of two sets of redundant equipment assemblies. The processor programs are included within the equipment in read only memory (firmware). One set of equipment is online and one standby, and has automatic and manual reconfiguration capability.

(5) The CCUs are interfaced to the Central Computer Complex Host (CCCH) by a General Purpose Input and General Purpose Output (GPI/GPO) adapter pair in the En Route Communication Gateway (ECG) equipment. The CCU is interfaced to the remote sites via modems and telephone lines or Remote Microwave Link (RML) to the RCUs or PC-RCUs.

b. POWER SUPPLIES.

(1) One or two dual single voltage power supplies, providing 5 Volts (V) and up to 12 ampere of direct current.

(2) Two or four dual multi-voltage power supplies, providing: 5 V at up to 12 amperes of direct current, 12 V at up to 1.7 amperes of direct current, and -12 V at up to 1.7 amperes of direct current.

c. MULTIBUS CARD CAGE ASSEMBLY. Each Multibus card cage assembly is a standard, 19-inch rack mountable assembly. The assembly contains a multibus back plane with four, 86-pin edge connectors. One of the edge connectors contains a single card microprocessor board, and one slot contains a utility board. The other two edge connectors are not used. The processor Printed Circuit Board (PCB) is an iSCB 88/45 Advanced Data Communications Processor board. The other board is a utility board, providing interface to CCCH system, expansion data memory, and the redundant control unit logic.

d. BUS CONNECTOR ASSEMBLY. The bus connector card cage assembly is a standard, 19-inch rack mountable assembly. The bus connector assembly contains a back plane with 16 edge connectors. This assembly can accommodate up to 16 bus connector PCBs. The bus connector boards provide a communications link between the Multibus assemblies and associated RCUs at terminal facilities.

202. FDIO-G**a. GENERAL.**

(1) The FDIO-G is located at the ARTCC. The FDIO-G replaces the legacy CCU. The FDIO-G routes data to and from a maximum of 64 remote sites. The FDIO-G will only interface with remote sites with a PC-RCU via FAA Telecommunication Infrastructure (FTI) or Bandwidth manager.

- (2) The FDIO–G consist of the following components:
 - (a) Two Flight Data Routers (FDR). Each FDR contains:
 - 1 Up to (4) Synchronous Serial Cards (SSC).
 - 2 One Cisco Ethernet Switch Interface Card (ESIC).
 - (b) A/B switching hardware which contains the following:
 - 1 One Remote Switching Router (RSR) with one (ESIC) card.
 - 2 Up to four Sycamore Network Intelligent Switch Patches (ISP), which contain:
 - a One power supply
 - b One control card
 - c Sixteen A/B switch cards
 - d One control converter
 - (c) One Lantronix Universal Device Server (UDS)
 - (d) Configuration laptop
 - (e) In-Rack Maintenance Switching system.
 - 1 One serial switch.
 - 2 One ethernet switch.
 - (f) Two 19–inch equipment racks with one APC Surge Arrest.

(3) The FDIO–G is interfaced to the CCCH through the Primary Interface Processor (PIP) or Backup Interface Processor (BIP) in the ECG. The interface from the ECG to the FDIO–G is Ethernet.

b. FDR.

(1) The FDR is a Cisco 3845 Integrated Service Router. It is a modular design router, which enables it to be configured for a wide area of applications. Within the FDIO–G system there are two FDRs, one for Network A that is designated FDR_A and one for Network B designated FDR_B.

(2) Each FDR has four Network Module Slots (NMS), four High Speed WAN Interface Cards (HWIC), two Gigabit Ethernet ports, and one console port. One Cisco Ethernet Switch Interface Card (ESIC) is installed in HWIC slot 0 to interface with the ECG PIP or BIP.

(3) **ESIC CARD IN FDR.** The ESIC provides the ability to connect four 10/100 BASE–T interfaces to each FDR . The ESIC provides layer 2 switching capability for data traffic between FDR and ECG. These interface connections are used to connect to ECG PIPA, PIPB, BIPA, and BIPB through the External LAN Switch (ELS). The interface adheres to Ethernet 802.11 specifications.

(4) **SSC.** The SSC provides the ability to connect 16 synchronous, RS–232 serial interfaces to the FDR. These serial interfaces provide the connectivity, thru telecommunication service, to the PC–RCU located at the remote sites. The Cisco smart serial cable that is connected to the serial port determines the mode of operation for the interface (DTE or DCE). For FDIO–G operation, DTE operation is used.

c. A/B SWITCHING HARDWARE. The A/B switching hardware is comprised of up to four ISPs chassis (ISP_1 through ISP_4), one Cisco 1841 router (RSR) and one Lantronix interface converter. This hardware provides ECG the capability to switch the serial data path, to remote site, between FDR_A and FDR_B.

(1) ISP.

(a) The ISP is a remotely or locally controlled A/B switching system, which provides for the switching of the physical RS–232 interface between the FDR_A and FDR_B to the PC–RCU. Each ISP is comprised of one chassis, one control card, one control converter, 16 A/B switch cards, and one power supply.

(b) The ISP can be either switched automatically by ECG, depending on the error condition, or manually. The A/B switch cards of the ISP use relay switching, which provides a physical connection between A/B sides and common. No data is buffered or electronically transferred by the switch card. The control card provides the means for controlling the ISP remotely or manually. A control converter is installed on the control card to provide the physical interface needed to connect the ISP to the Lantronix converter. ECG periodically requests status from the ISP to determine whether or not the ISP has been switched manually so the ECG has the current status.

(2) **RSR.** The RSR is a Cisco 1841 router, which provides the capability for connecting ECG (each PIP and BIP), to the ISPs. The RSR connects the ECG via Ethernet through the RSR ESIC. The RSR has one ESIC installed in slot 0 providing four Ethernet connections.

(3) **ESIC CARD IN THE RSR.** The ESIC provides the ability to connect four 10/100 BASE–T interfaces to the RSR. The ESIC provides the ability for layer 2 switching capability for data traffic between the RSR and ECG. These interface connections are used to connect ECG’s PIPA, PIPB, BIPA, and BIPB through the ELS switches. The interface adheres to Ethernet 802.11 specifications.

(4) **LANTRONIX UDS.** The Lantronix UDS converts incoming Ethernet packets from the ECG to RS–232 serial. The Lantronix is used to connect the RSR to the ISP.

d. CONFIGURATION LAPTOP. The configuration laptop is used to provide a means to connect to the FDRs and RSR for configuration and troubleshooting purposes. The laptop is a Commercial-off-the-Shelf (COTS) computer using Windows XP operating system. As such each site may have a different model, but it will provide the same functionality.

e. In-Rack Maintenance Switching. Provides two connections for the Configuration Laptop and each router for configuration, monitoring and maintenance. One connection is a serial connection from the Configuration Laptop through the serial Maintenance Switch to each router’s console port and to the Lantronix UDS. The second is an Ethernet connection from the Configuration Laptop through a 16/100 Ethernet switch to each router’s Ethernet port.

f. ECG CCU EMULATION SOFTWARE AND INTERFACES. With the replacement of the CCU with the FDIO–G, it was necessary for the ECG to absorb some of the CCU functionality as well as add new functionality to accommodate the new hardware architecture.

(1) A CCU Emulation Program (CCUAPP) is used within the ECG. Some of the responsibilities of the CCUAPP are as follows:

- IP address to HOST address mapping.
- EBCDIC to ASCII conversion.
- Message format conversion.
- Remote Switching.

(2) An Ethernet interface from ECG to FDIO–G was implemented. This interface replaces legacy GPO/GPI.

(3) A Point-to-Point Protocol (PPP) as the data link layer protocol on the serial interface has replaced the Advanced Data Communication Control Protocol (ADCCP). The Transmission Control Protocol (TCP), Internet Protocol (IP), and PPP are used to communicate between the ECG and the PC–RCUs.

203. RCUs.**a. GENERAL.**

(1) The RCU is located at the remote locations such as ATC Towers, TRACON facilities, and Military facilities. Each RCU controls and routes data to a maximum of 10 Replacement Flight Strip Printers (RFSP), 5 Replacement alphanumeric keyboards (RANK), and 5 Cathode Ray Tube (CRT) displays.

(2) The RCU consists of a single cabinet, which accommodates a 19-inch rack mounted electronic chassis. The cabinet contains two power supplies, one multibus processor and the number of bus connector assemblies required for that facility. There is no redundancy for the RCU equipment.

(3) The RCU equipment is interfaced via modems and telephone lines or RMLs to the CCU at the ARTCC or the S1R at the OFDPS.

b. POWER SUPPLIES.

(1) One single or one double power supply, providing 5 V and up to 12 amperes of direct current.

(2) One multi-voltage power supply, providing: 5 V at up to 12 amperes of direct current, 12 V at up to 1.7 amperes of direct current, and -12 V at up to 1.7 amperes of direct current.

c. MULTI BUS CARD CAGE ASSEMBLY. The Multibus card cage assembly is a standard, 19-inch rack mountable assembly. The assembly contains a multibus back plane with four, 86-pin edge connectors. One of the edge connectors contains a single card microprocessor board and one slot contains a memory expansion board. The other two edge connectors are not used. The processor PCB is an iSBC 88/45 Advanced Data Communications Processor Board. The other board is a 16 Kilobyte (KB) memory expansion board.

d. BUS CONNECTOR ASSEMBLY. The bus connector card cage assembly is a standard, 19-inch rack mountable assembly. The bus connector assembly contains a back plane with 16 edge connectors. This assembly can accommodate up to 16 bus connector PCBs. The bus connector boards provide a communications link between the Multibus assemblies and associated peripheral elements at the facility.

204. PC-RCU.

a. GENERAL.

(1) The PC-RCU replaces the functionality of the RCU. The PC-RCU system is located at the Terminal, Offshore, CERAP, and military facilities. Each PC-RCU system controls and routes data to a maximum of 10 RFSPs, 5 RANKs, and 5 CRTs, but the total number of peripherals cannot exceed 15. Although different models of PCs have been deployed, all provide the same FDIO functionality. The PC-RCU system consists of the following equipment either rack mounted or on pull out shelves:

(a) Dual processor (commercial processor, keyboard, and monitor).

(b) Ganged A/B switch.

(c) Dual surge protection.

(2) The PC-RCU consist of two PCs with VGA color monitor, keyboard, two or four peripheral interface boards with eight RS-422 asynchronous serial ports each, and two Qua-Tech, Inc. MPA-100 RS-232 synchronous communication boards. The PC-RCU software is loaded via a 3.5-inch floppy and saved to the hard drive.

(3) The redundant processor is a hot standby and is switched manually via the ganged A/B switch. There is no automatic switching between operational and redundant processors. The PC-RCU system has the capability to locally configure ports as "echo" ports. This is used to send flight plan data, destined to a local FDIO printer, to an external system (such as Tower Data Link Services (TDLS), Electronic Flight Strip Transfer System (EFSTS), etc). The PC-RCU system is interfaced via modems and telephone lines or RMLs to the CCU at the ARTCC or the S1R at the HCF facility (OFDPS) or the FDP at Anchorage ARTCC. The PC-RCU is also interfaced via telecommunication service to the FDIO-G at the ARTCC.

(4) FDIO software in the PC-RCU has the capability to be configured either as domestic or oceanic.

(a) The domestic terminal environment uses domestic software.

(b) Oceanic software is used in the PC-RCUs located in the OFDPS facilities, Hawaii Island terminals, and the San Juan CERAP.

(c) The domestic software provides one inch strips and the oceanic software provides one and one third inch strips.

Strip size:

Terminal (domestic)	1 inch
Terminal (Hawaii islands)	1 1/3 inch
OFDPS	1 1/3 inch
CERAP (San Juan)	1 1/3 inch

(5) The FDIO software in the PC–RCU has the capability to be configured to interface to the CCU using ADCCP protocol or FDIO–G using TCP/IP over PPP. The PC–RCU will detect the protocol received from the FDIO equipment at the ARTCC and automatically configure itself for the proper protocol.

b. GANGED A/B SWITCH. The ganged A/B switch consists of a power supply and A/B DB–9 cards (one for each peripheral plus one for the modem). The ganged A/B switch provides ganged switching capability for all FDIO peripherals and the site's interface modem from the operational to the redundant PC. Toggling one switch will switch all peripherals and modem to the redundant PC and the redundant PC will automatically become operational. The old operational PC will go to standby mode. No other action is required.

c. SURGE PROTECTION. Each PC has its own input power surge protection.

205. RFSP

The RFSP is used to print flight plan data. It prints user composed messages and logs error messages. One of two types of printers may be in use. The Data Products (FA 10095/11) dot matrix printer or the IER thermal printer (FA 10095/13). The IER printer is firmware controlled. The printer can be configured to produce a one or one and a third inch strip.

206. RANK.

This keyboard device is used to provide an operator interface for entering flight plan data into the system. One of two types may be in use: FA 10095/3 or FA 10095/17.

207. CRT.

The CRT is a peripheral element used to display flight plan messages, general information messages, weather data, and provides an area for composition and editing of input messages. The CRT could be one of two types. The FALCO CRT (FA 10095/12) or the ADDS CRT (FA 10095/18).

208. FDIO PERIPHERAL EMULATION.

Several external systems emulate the FDIO monitor and keyboard in the tower cabs. This is to reduce the number of peripherals in the tower cab or facility.

a. TDLS. The TDLS implements emulation of the FDIO RANKs and CRTs to reduce the number of keyboards and displays in the tower cabs. The FDIO RANK and CRT functions are shared with the pre-departure clearance terminal. The FDIO printer in the tower cab is not emulated in the TDLS system.

b. VISUAL INFORMATION DISPLAY SYSTEM (VIDS). The VIDS is a Navy system that implements emulation of FDIO RANK and CRT to reduce the number of peripherals in the Navy facility. The VIDS shares the functions of the FDIO CRT and keyboard with other Navy functions on their peripherals. The FDIO printer in the tower cab is not emulated in the VIDS.

c. OFDPS. The OFDPS emulates the FDIO RANK functions on a dual keyboard (Micro En Route Automated Radar Terminal System (MEARTS) and FDIO). The keyboard is part of the Enhanced Approach Radar Terminal System (EARTS).

209. FDIO EXTERNAL CONNECTIONS.

Several external programs (EFSTS, TDLS, ACE–IDS, and IDS) require flight plan data from selected tower/TRACON FDIO printers. If the facility has an RCU, the connection is via a special ‘Y’ cable at the peripheral output port of the RCU. The ‘Y’ cable allows one way communication only. If the facility has a PC–RCU, any unused port can be adapted as an ‘echo’ port to send the selected printer data to the external system. Facilities with a PC–RCU should not be using the ‘Y’ cable connection. If any are connected, coordinate with the external user and move it to an echo port.

210.–299. RESERVED.

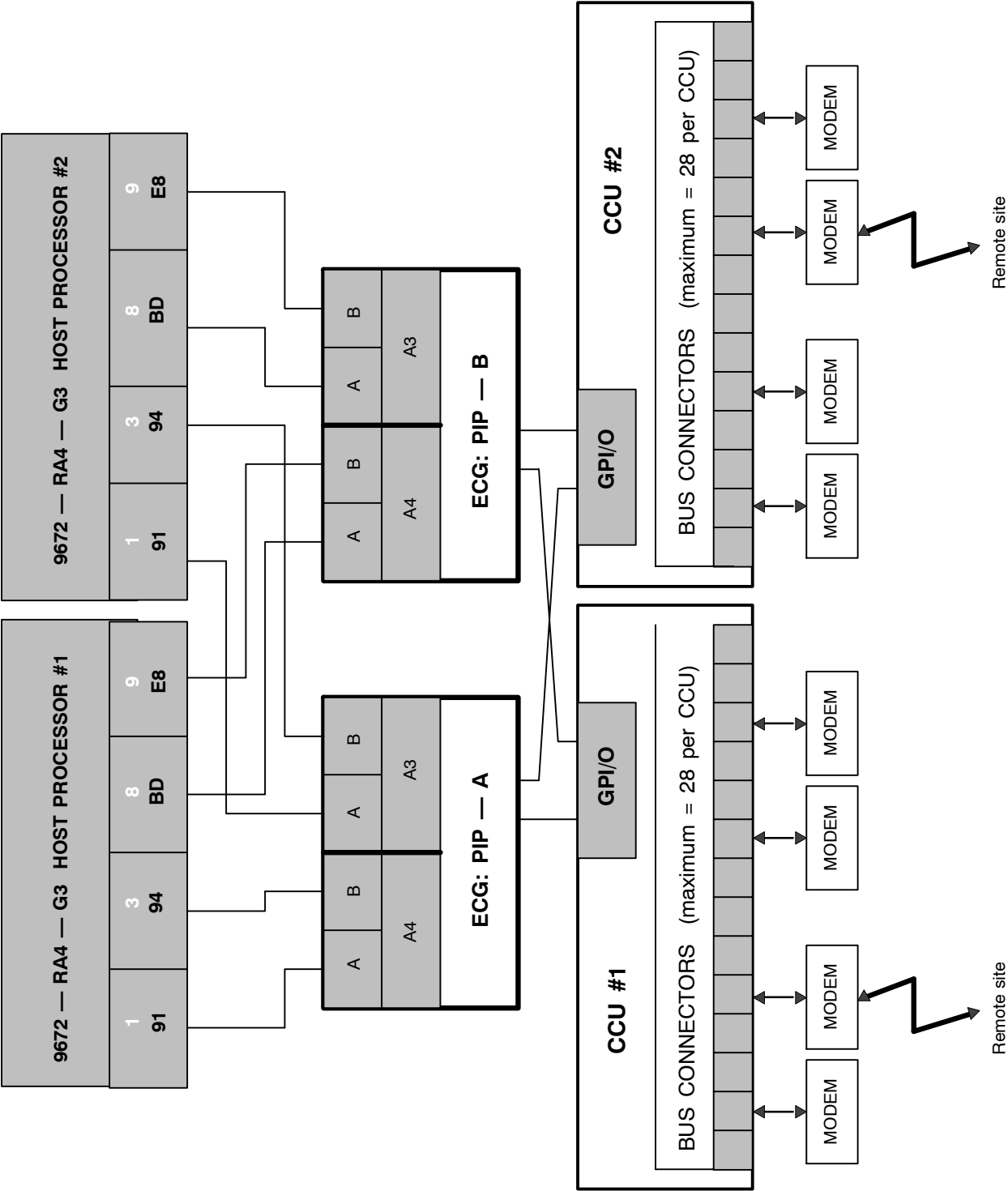


FIGURE 2-1. ARTCC FDIO SYSTEM FUNCTIONAL BLOCK DIAGRAM

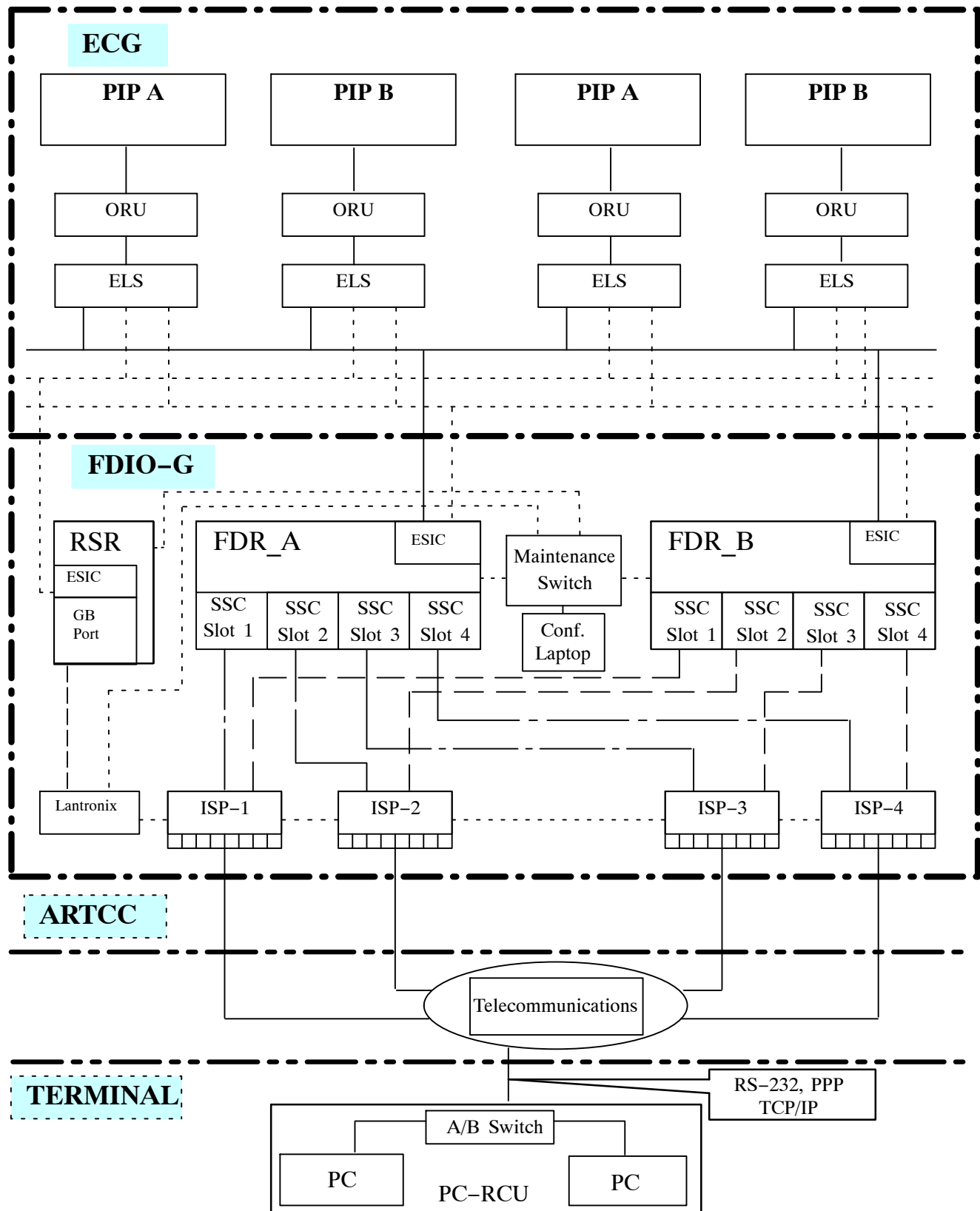


FIGURE 2-2. FDIO-G SYSTEM FUNCTIONAL BLOCK DIAGRAM

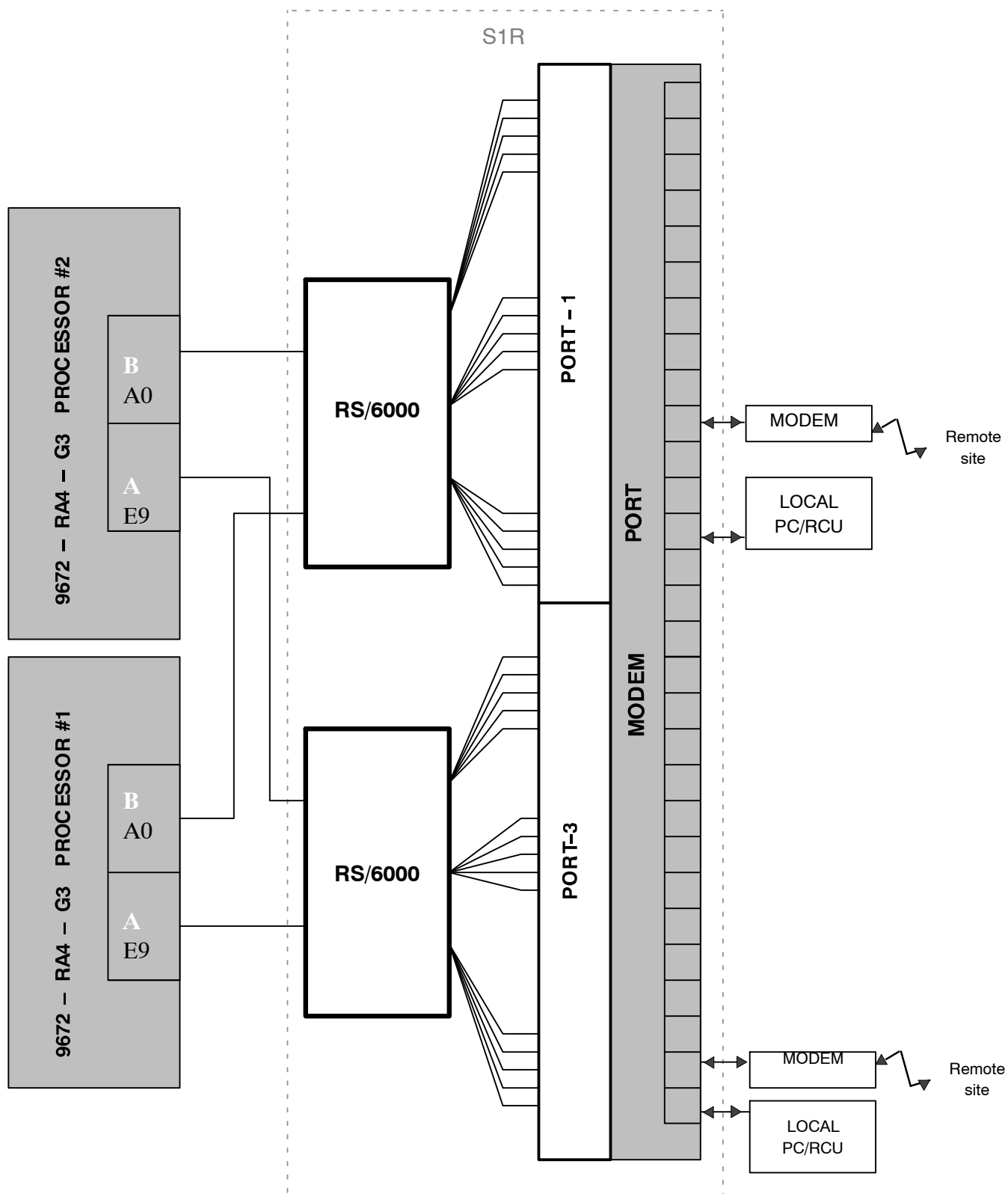


FIGURE 2-3. OFDPS (HCF) FDIO SYSTEM FUNCTIONAL BLOCK DIAGRAM

FDP2000 System

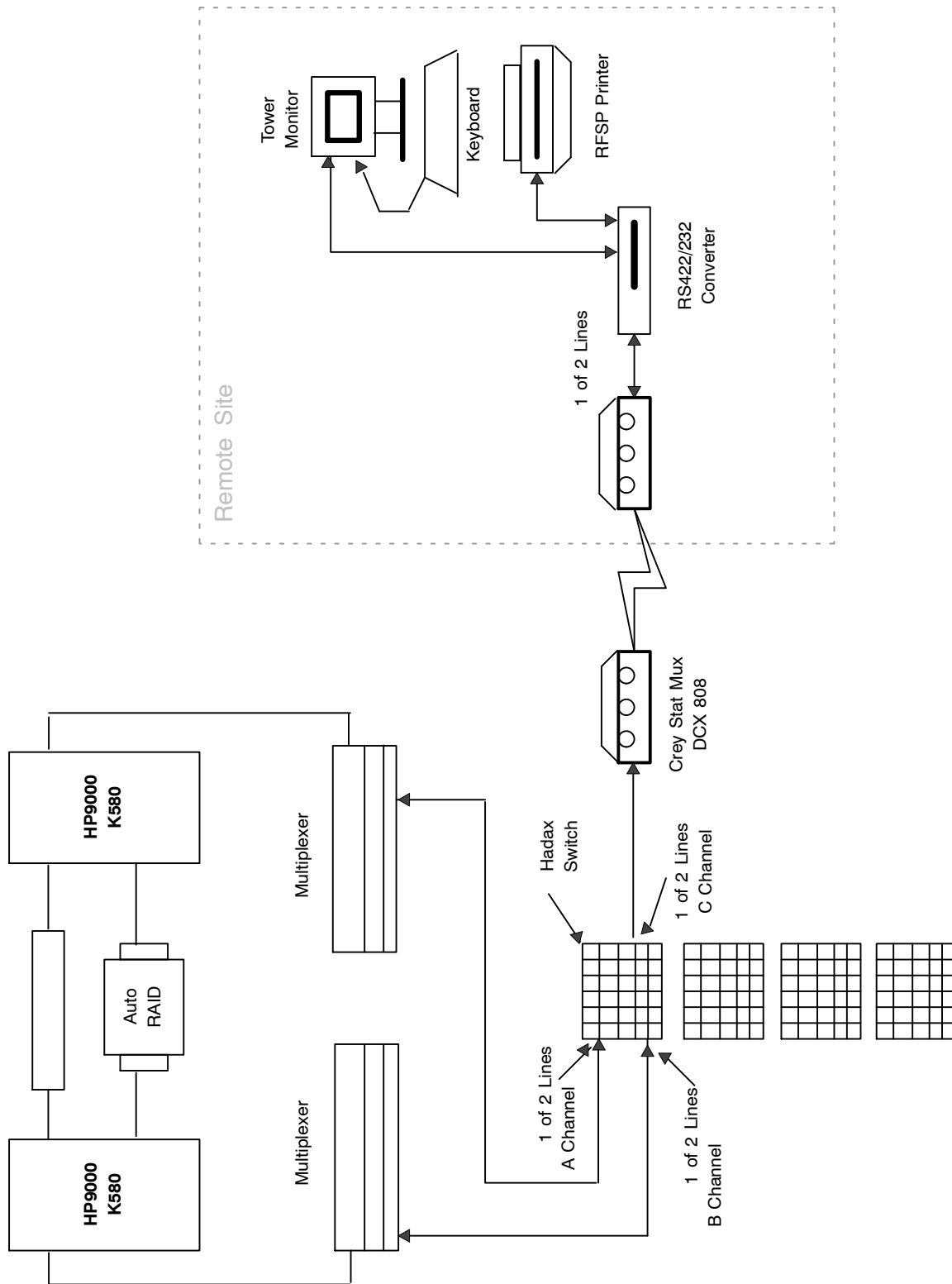
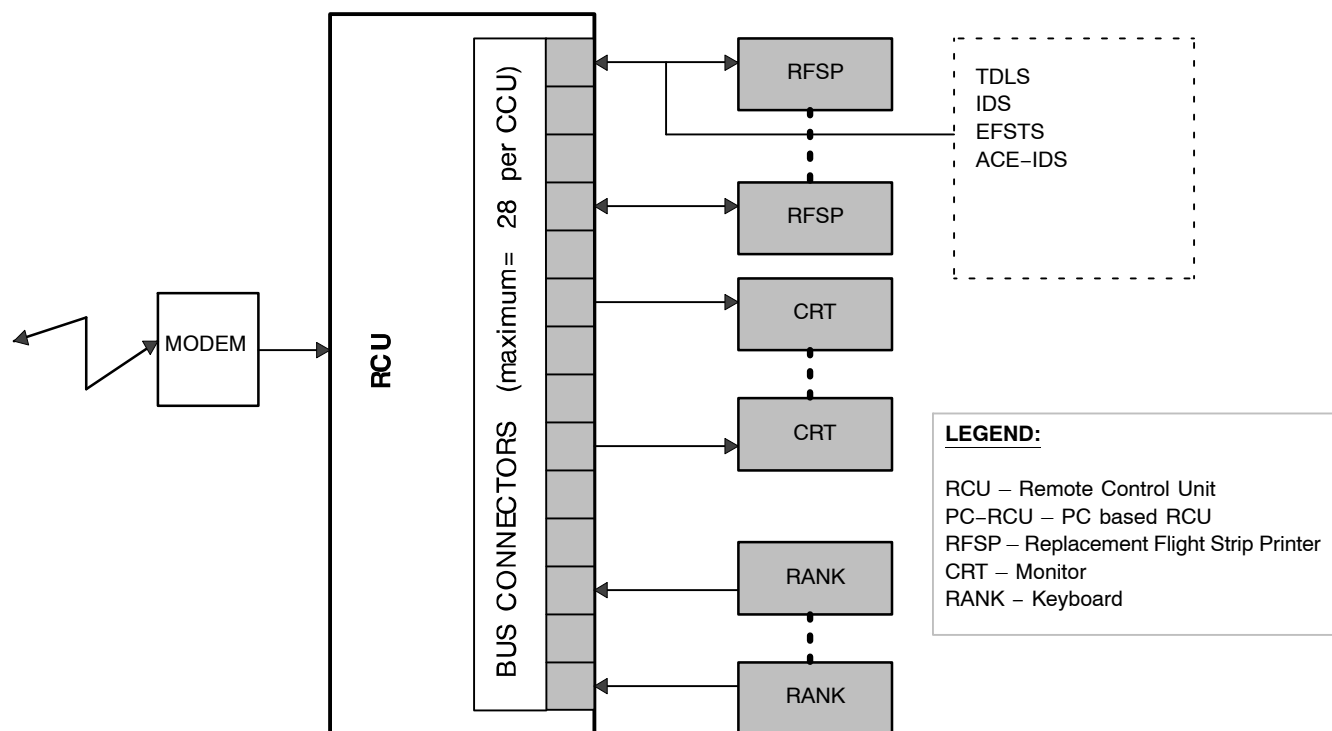


FIGURE 2-4. ALASKA FDIO SYSTEM FUNCTIONAL BLOCK DIAGRAM

TERMINAL SITE



TERMINAL/OFFSHORE SITE

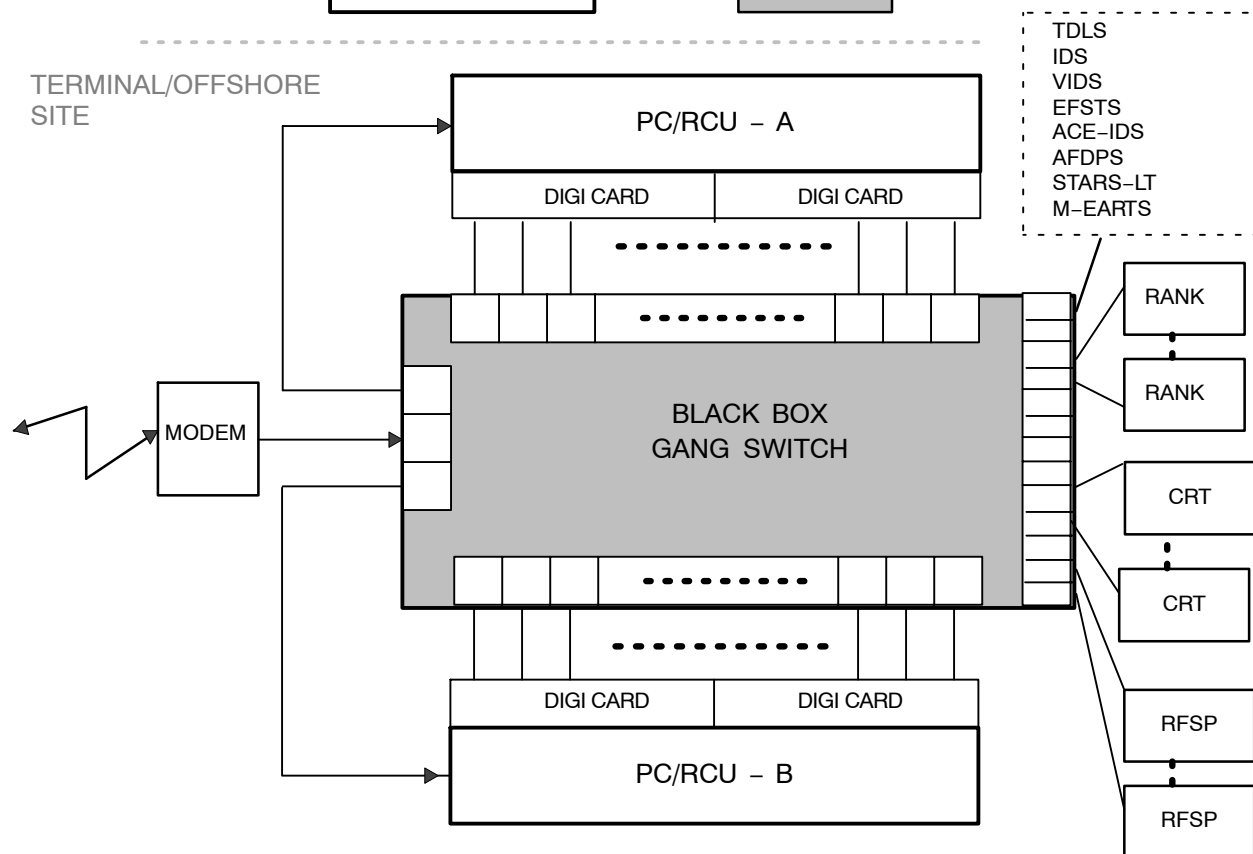


FIGURE 2-5. TERMINAL/OFFSHORE FDIO SYSTEM FUNCTIONAL BLOCK DIAGRAM

CHAPTER 3. STANDARDS AND TOLERANCES

300. GENERAL.

a. This chapter prescribes the standards and tolerances for FDIO equipment, as defined and described in Order 6000.15. All key performance parameters and/or key inspection elements are clearly identified by an arrow placed to the left of the applicable item.

b. Definitions of standard, initial tolerance, and operating tolerances for the purpose of this handbook are as follows:

- (1) **Standard.** The optimum value assigned to an essential parameter of the equipment.
- (2) **Initial Tolerance.** The maximum deviation, from the standard value of the parameter, which is permissible at the time of initial tune-up or a major readjustment.
- (3) **Operating Tolerance.** The maximum deviation, from the standard value of the parameter, beyond which remedial action by maintenance personnel is mandatory.

STANDARDS AND TOLERANCES

<i>Parameter</i>	<i>Reference Paragraph</i>	<i>Standard</i>	<i>Tolerance/Limit</i>	
			<i>Initial</i>	<i>Operating</i>
301. FDIO EQUIPMENT.				
a. ARTCC		Satisfactory input/output and transfer of flight data between remote site and ARTCC, including correct device response, as verified using online or offline certification programs, NAS TD message, or HOST online test tool "DIAG CCU".	None	None
b. Offshore.				
→ (1) HCF and Remote Site.		Satisfactory input/ output and transfer of flight data between HCF and remote site including correct device response as verified using online or offline certification programs or NAS TD message.	None	None
→ (2) OFDPS and Local Controller Position.		Satisfactory input/ output and transfer of data between OFDPS and local controller position, including correct device response, printer registration and print quality as verified using online/ offline certification programs or NAS TD message.	None	None
→ (3) Local Controller Keyboard and OFDPS.		Satisfactory transfer of data from the local controller keyboard to the OFDPS as verified using NAS TD message.	None	None

STANDARDS AND TOLERANCES (Continued)

<i>Parameter</i>	<i>Reference Paragraph</i>	<i>Standard</i>	<i>Tolerance/Limit</i>	
			<i>Initial</i>	<i>Operating</i>
c. Terminal		Satisfactory input output and transfer of flight data between the local controller and the ARTCC/HCF flight data processor including correct device response, registration and print quality as verified using NAS TD message.	None	None
302. CCU.	TI 6130.6, Par. 4.1			
a. +5 V Power Supply.		+5.0 V	± 0.01 V	± 0.1 V
b. +12 V Power Supply.		+12.0 V	± 0.06 V	± 0.6 V
c. -12 V Power Supply.		-12.0 V	± 0.06 V	± 0.6 V
d. Maximum Ripple Voltage at Power Supply.		0.25 V peak-to-peak	None	None
303. FDIO-G.				
a. Switch FDR		Error Free	Same as Standard	Same as Standard
b. FDR-Run Power-On ... Self Test (POST).		Error Free	Same as Standard	Same as Standard
c. RSR-Run POST		Error Free	Same as Standard	Same as Standard
d. Verify FDR and RSR to ECG redundant path.		Error Free	Same as Standard	Same as Standard

STANDARDS AND TOLERANCES (Continued)

<i>Parameter</i>	<i>Reference Paragraph</i>	<i>Standard</i>	<i>Tolerance/Limit</i>	
			<i>Initial</i>	<i>Operating</i>
304. RCU.	TI 6130.6, Par. 4.1			
a. +5 V Power Supply.		+5.0 V	± 0.01 V	± 0.1 V
b. +12 V Power Supply.		+12.0 V	± 0.06 V	± 0.6 V
c. -12 V Power Supply.		-12.0 V	± 0.06 V	± 0.6 V
d. Maximum Ripple Voltage at Power Supply.		0.25 V peak-to-peak	None	None
305. PC-RCU.				
a. Switch Control Units.		Error free	Same as Standard	Same as Standard
b. Run POST		Error free completion	Same as Standard	Same as Standard
306.-399. RESERVED.				

CHAPTER 4. PERIODIC MAINTENANCE

400. GENERAL.

a. This chapter establishes all the maintenance activities required for the FDIO equipment on a periodic, recurring basis, and the schedules for their accomplishment. The chapter is divided into two sections. The first section identifies the performance checks (i.e., tests, measurements, and observations) of normal operation controls and functions, which are necessary to determine whether operation is within established tolerances/limits. The second section identifies other tasks that are necessary to prevent deterioration and ensure reliable operation. Refer to Order 6000.15 for additional general guidance.

b. All reference paragraphs pertaining to standards and tolerance/limits are found in chapter 3 of this order, unless otherwise stated.

c. The performance checks and maintenance tasks are not to be taken as the minimum work required for proper maintenance, rather as the maximum interval permitted between task. This chapter will reference specific paragraphs for the maintenance activities listed in the individual equipment instruction books and their frequency of accomplishment.

d. Additional maintenance activities, not listed in the instruction books, will refer the user to chapter 5 of this handbook for the appropriate maintenance procedures.

Section 1. PERFORMANCE CHECKS (Continued)

<i>Performance Checks</i>	<i>Reference Paragraph</i>	
	<i>Standards & Tolerances</i>	<i>Maintenance Procedures</i>
402. FDIO–G.		
a. Monthly.		
Switch FDR	Par. 303a	TI 6130.6, Vol. 4 Par. 13.8.1.2
b. Quarterly.		
(1) Run FDR POST.	Par. 303b	TI 6130.6, Vol. 4 Par. 13.8.1.3
(2) Run RSR POST.	Par. 303c	TI 6130.6, Vol. 4 Par. 13.8.1.4
(3) Verify FDR and RSR to ECG redundant path.	Par. 303d	TI 6130.6, Vol. 4 Par. 13.8.1.1
403. PC–RCU.		
a. Monthly.		
Switch Control Units.	Par. 305a	TI 6130.6, Vol. 3 Par. 12.6.2.2
b. Quarterly.		
POST	Par. 305b	TI 6130.6, Vol. 3 Par. 12.6.2.3
404.–449. RESERVED.		

Section 2. OTHER MAINTENANCE CHECKS

<i>Maintenance Checks</i>	<i>Reference Paragraph</i>	
	<i>Standards & Tolerances</i>	<i>Maintenance Procedures</i>
450. FDIO EQUIPMENT.		
a. Monthly.		
(1) RFSP		
(a) Data Products		TI 6130.6, Vol. 1
<u>1</u> Clean exterior	None	Par. 6.4.7.1
<u>2</u> Vacuum interior	None	Par. 6.4.7.1
(b) IER Printer		TI 6130.6, Vol. 1
Clean print head and	None	Par. 6.4.7.2.1
platen.		
(2) RANK.		TI 6130.6, Vol. 1
(a) Clean exterior	None	Par. 6.4.6
(b) Verify lamp brightness	None	Par. 6.2.3
and control.		
(3) CRT.		TI 6130.6, Vol. 1
(a) Clean exterior.	None	Par. 6.4.5
(b) Clean screen.	None	Par. 6.4.5
(c) Verify contrast.	None	Par. 6.2.2
(d) Verify brightness.	None	Par. 6.2.2
b. Quarterly.		
(1) CCU.		TI 6130.6, Vol. 1
(a) Check power supply voltages.	Par. 302	Par. 6.3.2
(b) Check power supply ripple.	Par. 302	Par. 6.3.2.3.8

Section 2. OTHER MAINTENANCE CHECKS (Continued)

<i>Maintenance Checks</i>	<i>Reference Paragraph</i>	
	<i>Standards & Tolerances</i>	<i>Maintenance Procedures</i>
(2) RCU		TI 6130.6, Vol. 1
(a) Check power supply voltages.	Par. 304	Par. 6.3.2
(b) Check power supply ripple.	Par. 304	Par. 6.3.2.3.8
(3) PC–RCU.		
Verify fan operation in processors.	None	None
(4) FDIO–G.		
(a) Clean FDR fans	None	TI 6130.6, Vol. 4 Par. 13.8.2.2
(b) Verify RSR fan operation	None	None
c. Semiannually		
RFSP (IER)		TI 6130.6, Vol. 1
(1) Clean cutter blade, blade down sensor and interior.	None	Par. 6.4.7.2.2
NOTE: Semiannually or as indicated (Service) on the printer LED.		
(2) Platen roller brush cleaning.	None	TI 6130.6, Vol. 1 Par. 6.4.7.2.3
d. Annually		
(1) CCU.		TI 6130.6, Vol. 1
Clean interior and exterior.	None	Par. 6.4.1
(2) RCU.		TI 6130.6, Vol. 1
Clean interior and exterior.	None	Par. 6.4.1
(3) PC–RCU.		
Clean exterior.	None	TI 6130.6, Vol. 3 Par. 12.6.2.1

Section 2. OTHER MAINTENANCE CHECKS (Continued)

<i>Maintenance Checks</i>	<i>Reference Paragraph</i>	
	<i>Standards & Tolerances</i>	<i>Maintenance Procedures</i>
(4) FDIO–G.		
(a) FDR.		
Clean exterior	None	TI 6130.6, Vol. 4 Par. 13.8.2.2
(b) RSR.		
Clean exterior	None	TI 6130.6, Vol. 4 Par. 13.8.2.3
(c) ISP.		
Clean exterior	None	TI 6130.6, Vol. 4 Par. 13.8.2.4
(d) Laptop.		
Clean exterior	None	TI 6130.6, Vol. 4 Par. 13.8.2.5
451.–499. RESERVED.		

CHAPTER 5. MAINTENANCE PROCEDURES

500. GENERAL.

This chapter establishes the procedures for accomplishing the various essential maintenance activities which are required for the FDIO equipment, on either a periodic or incidental basis. The chapter is divided into three sections. The first section describes the procedures to be used in making the performance checks listed in chapter 4, section 1. The second section describes the procedures for doing the tasks listed in chapter 4, section 2. The third section describes procedures for doing special tasks, usually nonscheduled and not listed in chapter 4. Refer to Order 6000.15 for additional general guidance.

Section 1. PERFORMANCE CHECK PROCEDURES

501. GENERAL PERFORMANCE CHECK PROCEDURES.

All other performance checking procedures, and other guidance essential to maintaining continuous error free operation of the FDIO equipment is found in TI 6130.6.

502. TD PROCEDURE FOR THE EN ROUTE CENTER, TERMINAL, OR OFDPS FACILITY.

a. **Object.** Verify FDIO operation.

b. **Description.** This procedure will cause a TD message to be sent to the requested peripheral. This will test the FDIO interface and verify the correct operation of the printer.

c. **Test Equipment Required.** None.

d. **Condition.** Systems must be operational and interfaced.

e. **Detailed procedure.**

Enter the following TD command for the position being tested.

TD aaaL or TD aaaLbbb

(1) Where aaa is the identifier for the tower or approach control facility.

(2) Where L is replaced with T for tower printer, with D for approach control departure printer, with A for approach control arrival printer, and with O for approach control over flight printer.

(3) Where bbb is required only if a printer name is adapted for an approach control departure or arrival printer.

NOTE: Refer to NAS–MD–311, paragraph 8.5 for complete format.

503. TD PROCEDURE FOR FDIO PRINTERS AND CRTS AT THE OFDPS FACILITY.

a. **Object.** Verify FDIO operation.

b. **Description.** This procedure will cause a TD message to be sent to the requested peripheral. This will test the interface and verify the correct operation of the printer or CRT.

c. **Test Equipment Required.** None.

d. **Condition.** System must be operational.

e. **Detailed procedure.**

From the FDIO keyboard enter the following TD command for the peripheral being tested.

TD P or TD

(1) Where P will cause the TD message to print on the printer associated with the keyboard.

(2) If the P does not follow the TD, the TD message will be displayed on the CRT associated with the keyboard.

NOTE: Refer to NAS–MD–311 for complete details.

504. TD PROCEDURE FOR THE ALASKA CENTER TO TERMINAL FACILITY.

a. Object. Verify FDIO operation.

b. Description. This procedure will cause a TD message to be sent to the requested terminal printer. This will test the interface and verify the correct operation of the FDIO interface and printer.

c. Test Equipment Required. None.

d. Condition. System must be operational.

e. Detailed procedure.

Enter the following TD command for the facility being tested.

TD sss

(1) Where sss is the sector number of the printer where the message will be printed.

(2) If the sector number is omitted, and the entering source is not a supervisory position, the TD message will be printed on the printer associated with the keyboard from which the TD was entered.

(3) If the TD is entered at a supervisory station and the sector number is omitted, the TD message will be printed on all printers.

505.–539. RESERVED.

Section 2. OTHER MAINTENANCE TASKS

540. GENERAL MAINTENANCE TASKS.

All other maintenance task procedures for the FDIO equipment is found in TI 6130.6. Housekeeping tasks such as equipment cleaning and the changing of filters, lubrication of motors, and the like, are covered in Order 6000.15.

541.–569. RESERVED.

Section 3. SPECIAL MAINTENANCE PROCEDURES

570.–599. RESERVED.

APPENDIX 1. CERTIFICATION REQUIREMENTS

Refer to Order 6000.15, Appendix 3, for the list of constituent NAS, and for general guidance on the certification of services and systems.

NOTE: No certification is required for the FDIO hardware system. Service certification, if required, is the responsibility of the ARTCCs and Offshore (HCF) facilities. Personnel at these facilities should refer to the latest version of Orders 6100.1 and 6110.8 for requirements.

APPENDIX 2. GLOSSARY OF TERMS AND ABBREVIATIONS

Alphanumeric	A combination of alphabetic and numeric characters.
Central Computer	The physical components of the 3083 IBM computer and its associated peripheral equipment.
Equipment, Peripheral	The auxiliary machines which may be placed under the control of a control unit. Examples of this are keyboards, monitors, printers.
Interface	The common boundary of two bodies or spaces. The functional intersystem relationship which influence system accomplishments.
Keyboard	A computer entry device used to enter messages into the computer for processing.
Message	A group of words transported as a unit.
Modem	Modulating and demodulating (communication equipment).
National Airspace System	The common system of facilities, equipment regulations, procedures, and personnel required for the safe and efficient movement of civil and military aircraft in airspace within the jurisdiction of the United States.
Offline	In computer language, pertaining to auxiliary equipment or output device not under control of the central processing unit.
Online	In computer language, pertaining to operation of devices under direct control of the computer.
Operational Equipment	Equipment that is in actual use for air traffic control.
Output Equipment	The equipment used to transfer information out of a computer.
Software	In computer terminology, all the programming systems required for effective data processing operations.
Subsystem	An essential, functional part of a system which supports a data processing operation.
System Support	The engineering model computer installation and overhead facility located at the FAA Technical Center.

APPENDIX 3. ABBREVIATIONS

ACE–IDS	Automated Surface Observing System Controller Equipment– Information Display System
ADCCP	Advanced Data Communication Control Protocol
ARTCC	Air Route Traffic Control Center
ARTS	Approach Radar Terminal System
AT	Air Traffic
ATA/IDE	Advanced Technology Attachment/ Intergrated Drive Electronics
ATC	Air Traffic Control
ATCT	Air Traffic Control
ATO	Air Traffic Organization
BIP	Backup Interface Processor
BIOS	Basic Input Output System
CCCH	Central Computer Complex Host
CCD	Configuration Control Decision
CCU	Central Control Unit
CCUAPP	CCU Emulation Program
CERAP	Center Radar Approach Control
CM	Configuration Management
COTS	Commercial–Off–The–Shelf
CRT	Cathode Ray Tube
CSIC	Cisco Ethernet Switch Interface Card
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DoD	Department of Defence
DOT	Department of Transportation
EARTS	Enhanced Approach Radar Terminal System
ECG	En Route Communication Gateway

EFSTS	Electronic Flight Strip Transfer System
ELS	Extended LAN Switch
ESIC	Ethernet Switch Interface Card
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FDIO	Flight Data Input/Output
FDIO–G	Flight Data Input/Output Gateway
FDP	Flight Data Processor
FDR	Flight Data Router
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTI	FAA Telecommunication Infrastructure
GPI	General Purpose Input
GPO	General Purpose Output
HCF	Honolulu Control Facility
HWIC	High Speed WAN Interface Card
IAW	In Accordance with
ID	Identification
IDS	Information Display System
IER	Name of Printer Manufacture
IP	Internet Protocol
ISP	Intelligent Switch Patch
ISSO	Information System Security Officer
KB	Kilobyte
KYBD	Keyboard
LAN	Local Area Network
LED	Light Emitting Diode
LES	Law Enforcement Sensitive
M–EARTS	Micro En Route Automated Radar Tracking System
NAPRS	National Airspace Performance Reporting System
NAS	National Airspace System

NCP	NAS Changer Proposal
NOM	NAS Operations Manager
NMS	Network Module Slots
NSA	National Security Agency
NSCT	NAS Certification Tape
OFDPS	Offshore Flight Data Processing System
OLC	Online Certification
ORU	Operational Router Unit
OS	Operating System
OUO	Official Use Only
Par.	Paragraph
PC	Personal Computer
PCB	Printed Circuit Board
PCII	Protected Critical Infrastructure Information
PC-RCU	Personal Computer-Remote Control Unit
PIP	Primary Interface Processor
POST	Power-On-Self Test
PPP	Point-to-Point Protocol
RANK	Replacement Alphanumeric keyboard
RCU	Remote Control Unit
RFSP	Replacement Flight Strip Printer
RML	Remote Microwave Link
RSR	Remote Switch Router
S1R	Series/1 Replacement
SBU	Sensitive But Unclassified
SCSI	Small Computer System Interface
SHSI	Sensitive Homeland Security Information
SSC	Synchronous Serial Card
SSE	Servicing Security Element
SSI	Sensitive Security Information
STARS-LT	Standard Terminal Automation Replacement System-LITE

SUI	Sensitive Unclassified Information
TCP	Transmission Control Protocol
TD	Test Device
TDLS	Tower Data Link Services
TOS	Technical Operations Services
TRACON	Tower Radar Approach Control
UDS	Universal Device Service
V	Volts
VGA	Video Graphic Array
VIDS	Visual Information Display System
WAN	Wide Area Network
WJHTC	William J. Hughes Technical Center

APPENDIX 4. SENSITIVE SECURITY INFORMATION AND MAGNETIC MEDIA DISPOSAL/REUTILIZATION POLICY/PROCEDURES

1. PURPOSE.

This appendix provides guidance to TOS employees who have a requirement to dispose of, or reuse, unclassified computer storage media that contains Sensitive Security Information (SSI) or For Official Use Only (FOUO) information. These procedures do not pertain to any Classified (i.e., Secret, Top Secret) media.

2. SCOPE.

These procedures pertain to any Sensitive But Unclassified (SBU) data contained on hard drives, disk drives, and any other type of computer storage media under the purview of the FAA that contains SSI or FOUO information. Computer storage media located at FAA site(s), but owned or managed by other government agencies (i.e., Department of Defense (DoD), Federal Bureau of Investigation (FBI)), will not use these procedures, but will follow the procedures and/or guidelines for reusing or destroying magnetic media dictated by that particular agency. If the storage media is FAA-owned but contains sensitive information from another outside agency (i.e., DoD), then the sanitization procedures from the outside agency must be followed. If the outside agency's procedures are determined by the division ISSO to be better than or equal to the procedures outlined in this appendix, then no other action is necessary. If the outside agency's procedures are unknown or less stringent, then the procedures outlined in this appendix should be utilized.

3. BACKGROUND.

Computer storage media that contains SBU information cannot be reused or excessed unless all information has been destroyed or removed beyond comprehension. Reformatting the drive or deleting files will not completely remove the data from a system. There is still a great chance that the data can be recovered.

A number of methods can be used to accomplish proper sanitization. This document will provide three sets of procedures that will satisfy requirements necessary for reusing or disposing of electronic storage media. These procedures are:

- a. overwriting the data manually and/or using approved data-overwriting software,
- b. degaussing (i.e., demagnetizing the data), and
- c. destroying the media.

4. POLICY.

In accordance with requirements stated in the latest edition of Order 1370.82, Information Systems Security Program, to maintain the confidentiality and accountability of sensitive information, TOS FAA and support contractor personnel shall ensure confidentiality of sensitive data when reusing or disposing of magnetic media. The procedures contained in this document shall be followed when disposing of, or reusing, unclassified computer storage media that contains SSI and/or FOUO information. Authority to destroy magnetic media must be obtained from the owner or Property Custodian, whichever is appropriate, prior to executing any procedure that destroys data or the media.

All personnel shall follow the latest edition of Order 1600.2, Safeguarding Classified national Security Information, when disposing or reusing magnetic media that contains classified information.

5. PROCEDURES FOR SANITIZING SBU ELECTRONIC STORAGE MEDIA.

Any one of the following procedures can be used when sanitizing any SBU electronic storage media before reuse or disposal. Before SBU media is to be removed or reused, the Division ISSO must be notified and consulted.

a. Overwriting Electronic Storage Media for Sanitization.

Overwriting is the process of replacing information (data) with meaningless data in such a way that the meaningful information cannot be recovered. The individual performing the overwriting will be responsible for certifying that the process has been successfully completed.

The process of overwriting data must be correctly understood and carefully implemented to be effective. Overwriting consists of recording data onto magnetic media by writing a pattern of binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, eight (8) of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., 11111111" followed by 00000000") the magnetic fluxes will be physically changed and the drive's read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge a hard drive requires overwriting with a pattern and then its complement, and finally with another pattern (e.g., overwrite first with _00110101," followed by 11001010" then 10010111"). Sanitization is not complete until all six passes of the three cycles are completed.

b. Data-overwriting Software.

Another method for sanitizing storage media is using commercial software. Certain software can be used but it must meet the criteria listed below, Paragraph 7, Acceptable Commercial Software Products, of this appendix. Software products and applications not meeting the stated minimum specifications are not acceptable for sanitizing SBU storage media. Overwriting software that reformats or repartitions a hard drive will not be accepted within the scope of this policy. Also, some software product versions may not have the capability to remove the Operating System (OS) during the overwrite process. To ensure the integrity of the sanitization process, overwriting software must have the following functions and capabilities:

- (1) The ability to purge all data or information, including the OS, from the physical or virtual drives, thereby making it impossible to recover any meaningful data by keyboard or laboratory attack,
- (2) A compatibility with, or capability to run independent of, the OS loaded on the hard drive,
- (3) A compatibility with, or capability to run independent of, the type of hard drive being sanitized (e.g., ATA/IDE or Small Computer System Interface (SCSI) type hard drives),
- (4) A capability to overwrite the entire hard disk drive independent of any Basic Input Output System (BIOS) or firmware capacity limitation that the system may have,
- (5) A capability to overwrite using a minimum of three cycles (six passes) of data patterns on all sectors, blocks, tracks, and slack or unused disk space on the entire hard disk medium,
- (6) A method to verify that all data has been removed from the entire hard drive and to review the overwrite pattern.

c. Degaussing.

Degaussing is a procedure that reduces the magnetic flux of a medium to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously-stored data on magnetic media unreadable. The drawback to degaussing is that very seldom can a drive be used after this process. For a degausser to be effective here are a few standards and procedures which must be used:

- (1) Degaussers used on FAA hard drives must have a nominal rating of at least 1700 Oersted.
- (2) Degaussers must be operated at their full magnetic strength.
- (3) The product manufacturer's directions must be carefully followed. Deviations from an approved method or rate of coercivity could leave significant portions of data remaining on a hard drive.
- (4) All shielding materials (e.g., castings, cabinets, and mounting brackets) which may interfere with the degausser's magnetic field must be removed from the hard drive before degaussing.

(5) Hard disk platters must be in a horizontal direction during the degaussing process.

(6) For degaussing hard drives with very high coercivity ratings, it may be necessary to remove the magnetic platters from the hard drive's housing.

(7) Degaussing products should be acquired from the National Security Agency's (NSA) Degausser Products List which can be obtained by contacting:

National Security Agency
Attn: S7 Media Technology Center
9800 Savage Road, Ft. George G. Meade, MD
20755-6877
Tel: 1 (800) 688-6115 (Option #3) or 1 (410)
854-7661
Fax: 1 (410) 854-7668.

d. Destruction of Media.

Destruction of media is generally used when a disk has damaged or unusable tracks and sectors and the disk is not reusable. Authority to destroy the media must be obtained from the Property Custodian before proceeding. Destruction of storage media is the process of physically damaging a medium so that it is not usable in a computer, and so that no known exploitation method can retrieve data from it. If possible, operable media should be overwritten or degaussed prior to destruction. The three acceptable methods of destruction are:

(1) Physical destruction/impairment beyond reasonable use: Remove the hard drive from the chassis or cabinet. Remove any steel shielding materials, mounting brackets, and cut any electrical connection to the hard drive unit. In a suitable facility with individuals wearing appropriate safety equipment, subject the hard drive to physical force (i.e., pounding with a sledgehammer) that will disfigure, bend, mangle, or otherwise mutilate the hard drive so that it cannot be re-inserted into a functioning computer. Sufficient force should be used directly on top of the hard drive unit to cause shock/damage to the disk surfaces. In addition, any connectors that interface into the computer must be mangled, bent, or otherwise damaged to the point that the hard drive could not be re-connected without significant rework.

(2) Destruction at a metal destruction facility, (i.e., smelting, disintegration, or pulverization).

(3) Application of an abrasive substance (emery wheel or disk sander) to a magnetic disk or drum recording surface. Make certain that the entire recording surface is completely removed. Ensure proper safety measures, to include protection from inhaling abraded dust and use of protective eyewear.

6. DEFINITIONS.

a. Clearing – Rendering stored information unrecoverable unless special utility software or techniques are used.

b. Degaussing – Reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used as a method of sanitization.

c. Media – Short for storage media. Physical objects on which data can be stored, such as hard drives, floppy disks, CD-ROMs, and tapes.

d. Overwriting – Process of writing patterns of data on top of the data stored on a magnetic medium.

e. Oerstad – A unit of magnetic field strength.

f. Sanitize – To expunge data from storage media so that data recovery is impossible. Sanitizing includes overwriting, degaussing, and destruction (destruction is not an appropriate means for TOS purposes). Clearing data does not constitute sanitizing.

g. SBU Information – SBU information is any information the loss, misuse, or unauthorized access to, or modification of, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine FAA payroll, finance, logistics, and personnel management systems.

7. ACCEPTABLE COMMERCIAL SOFTWARE PRODUCTS.

The following commercial software is of acceptable use for overwriting computer storage media. This is not to be considered an all-inclusive list, as there are other products that meet the minimum requirements, but this list should be used as a reference. This list is subject to change and should only be used as a reference.

- a.** Product Name: – No Trace™
Communication Technologies, Inc.,
14151 Newbrook Dr., Suite 400, Herndon,
VA 20170
Tel: (703) 961–9080
www.comtechnologies.com
- b.** Product Name: – DataEraser™
ONTRACK Data International, Inc.
Tel: 1 (800) 872–2599
www.ontrack.com
- c.** Product Name: – UniShred Pro™
Los Altos Technologies
Tel: (919) 233–9889
www.lat.com
- d.** Product Name: CleanDrive™
Access Data Corporation
(800) 574–5199
www.accessdata.com
- e.** Product Name: – Sanitizer D 4.01™
Infraworks
(512) 583–5000
www.infraworks.com/products/sanitizer.html

APPENDIX 5. POLICY/PROCEDURES FOR IDENTIFYING, HANDLING, MARKING AND DISPOSAL OF SENSITIVE UNCLASSIFIED INFORMATION (SUI)

1. PURPOSE.

This appendix provides guidance to employees regarding the rules and practices for identification, handling, marking, storage and disposal of media that contains FOUO information, SSI, Sensitive Homeland Security Information (SHSI) and/or Protected Critical Infrastructure Information (PCII). This guidance does not pertain to any Classified (i.e., Confidential, Secret, and Top Secret) media.

2. SCOPE.

This guidance pertains to any Sensitive Unclassified Information (SUI) discussed verbally, transmitted electronically, existent or generated as printed material and/or contained on hard drives, disk drives, and/or any other type of computer storage media under the purview of the FAA. It pertains to every FAA employee, contractor, consultant and grantee creating, handling, or accessing SUI.

3. BACKGROUND.

In the aftermath of September 11, 2001, there is a heightened awareness of the need to safeguard sensitive Government information that does not meet the standards for classified national security information. Of particular concern is the need to protect Government information related to homeland security. This includes information that supports the FAA global aerospace structure that contributes to the security of the nation and public safety. It is incumbent upon all FAA associated personnel to support these safeguards through increased awareness of the nature of such material and their duties and responsibilities for its protection.

4. POLICY.

In accordance with (IAW) requirements stated in the latest edition of Order 1600.75, Protecting Sensitive Unclassified Information (SUI), SUI is unclassified information – *in any form including print, electronic, visual, or aural forms* – that must be protected from uncontrolled release to persons outside the FAA and indiscriminate dissemination within the FAA. It includes aviation security, homeland security, and protected critical infrastructure information. SUI may include information that may qualify for withholding from the public under the Freedom of Information Act (FOIA). All personnel shall be aware of and follow the policies and procedures contained herein and in the latest edition of Order 1600.75. If conflicting guidance is provided, comply with Order 1600.75

5. TYPES OF SUI

Throughout the Federal Government there are more than 50 types of SUI. Within the FAA, only four types are generally encountered or handled:

a. FOUO information. FOUO is the primary designation given to SUI by the Department of Transportation (DOT) and FAA. It consists of information that could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals if released to unauthorized individuals. As examples, the uncontrolled use of FOUO information may allow someone to:

- (1) Circumvent agency laws, regulations, legal standards, or security protective measures

or

- (2) Obtain unauthorized access to an information system.

b. SSI. SSI is a designation *unique* to the DOT and DOT's operating administrations and to the Department of Homeland Security (DHS). It applies to information we obtain or develop while conducting *security activities*, including research and development activities. Unauthorized disclosure of SSI would:

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person;

or

(3) Be detrimental to transportation safety or security.

c. SHSI. SHSI is a designation *unique* to homeland security information that we share with State and local personnel. The Federal government shares SHSI with State and local personnel who are involved in prevention against, preparation for, or response to terrorism. We protect it because its loss, misuse, unauthorized disclosure or access, or modification can significantly impair the capabilities and efforts of Federal, State, and local personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of terrorism. If our sensitive unclassified information impairs these capabilities, we must designate it SHSI before we share it with State and local personnel to facilitate its proper protection.

d. PCII. PCII is a designation *unique* to critical infrastructure information provided by non-government persons and entities to the DHS. DHS uses the information for security of critical infrastructure and protected systems, analysis, warning, interdependency studies, recovery, reconstitution, or other informational purposes. While only DHS can designate information as PCII, they can share it with other Federal agencies as needed for operational purposes. PCII is defined in 6 CFR Part 29.

6. IDENTIFYING AND WORKING WITH SUI

Personnel working with this system are most likely to encounter SUI identified above. However, other Federal agencies use different terminology and markings to designate SUI. For example, the Department of Energy uses Official Use Only (OUO), the Department of State uses SBU, and the Drug Enforcement Administration uses DEA Sensitive. Many Federal law enforcement agencies use the term Law Enforcement Sensitive (LES). If an unfamiliar security designation is encountered, contact the SSE for guidance; treat the information in question as FOUO until specific resolution is obtained.

Most existent SUI will be marked accordingly. However, marking is not conclusive proof of sensitivity. Information sensitivity may cease because of the passage of time or change in circumstances. Also, because of error or changing sensitivities, unmarked SUI that should be marked or information that is marked but is no longer sensitive may be encountered. If there is any uncertainty about markings, contact the supporting SSE for a resolution and protect the questioned information as though it were FOUO information pending resolution.

The systems under cognizance of AJE-12, their operating systems and operational and backup data typically fall outside the scope of designation as SUI. However, the following specific information associated with AJE-12 programs and systems is considered SUI:

a. Lists and/or data files of employees and their respective system passwords or access codes. (FOUO)

b. System specific security information. (FOUO)

c. Procurement, grant, budget and other financial information and data. (FOUO)

d. Files and/or data bases containing specific private employee information such as medical histories, SSNs, personnel evaluations, etc. (SSI)

e. System or organizational vulnerability assessments. (SSI)

f. COOP documentation. (SSI)

- g.** SCAP documentation. (SSI)
- h.** Contingency planning documents, such as Disaster Recovery Plans. (SSI)
- i.** Trade secret or proprietary corporate information supplied in proposals and/or provided to the FAA under contract license agreements. (SSI)

A comprehensive, but generic listing of the specific information comprising SSI is provided in Order 1600.75, appendix A.

7. MARKING/LABELING SUI

Marking is a basic protective measure that draws a reader's attention to the sensitivity of information and the need to protect it. Marking aids in making disclosure decisions and selecting and applying appropriate protective measures.

All personnel are required to properly mark information when created or it is determined that it meets the standards of sensitive unclassified information. Exceptions:

a. Records in storage. If there are unmarked records in storage that should be marked, they need not be removed from storage only to mark them. Mark them when removed from storage for other purposes other than destruction. Stored documents slated for destruction need not be marked prior to destruction provided the individual removing the document from storage can ensure destruction is accomplished as specified in paragraph 10 of this appendix.

b. Records marked under old authority. Information marked under an old regulatory authority, e.g., 14 CFR § 191 for Sensitive Security Information may be marked differently than directed by this order. Remark-ing these documents is not required.

c. Sensitive non-government information. Your office may receive information from contractors, grantees, businesses, and regulated parties marked as business sensitive, company confidential, proprietary, trade secret, and so on. Remarking this information is not required, but it must be protected from unauthorized disclosure. Unless greater protective measures are specified by the information's originator, protect it as FOUO information.

Refer to Order 1600.75, appendixes D and E for the most current guidance for marking FOUO information and SSI, which have different marking protocols. The SHSI Program Officer and PCII Officer will issue separate marking guidance for SHSI and PCII.

When marking documents and other material containing both classified national security information and SUI, refer to FAA Order 1600.2.

Mark other records, such as photographs, films, tapes, slides, or records residing in information systems with appropriate protective markings and distribution limitation statements in a conspicuous way so that persons having access to them are aware of their sensitivity.

Mark removable electronic media, e.g., diskettes and compact disks, with the appropriate protective marking and distribution limitation statement in a conspicuous way so that persons having access to them are aware of their sensitivity. The System ISSP will contain additional specific measures for labeling and marking removable media.

8. STORING SUI

a. During Working Hours

(1) Physical custody or control. When SUI is not in secure storage, it must be under the protection and control of an authorized person.

(2) Not under physical custody or control. When your SUI is not under the physical custody or control of an authorized person, you must store it in a lockable container, such as a file cabinet or desk,

or in a locked space. Your office must control the keys to the locks of these containers and spaces, and key holders must be authorized persons.

b. After Working Hours

(1) **Uncontrolled work spaces.** If the work area is accessible to persons, who are not authorized access to the SUI, it must be stored in a secure container such as a locked desk, file cabinet, or an inaccessible locked space. The sub-team office must control the keys to the locks of these containers and spaces, and key holders must be authorized persons.

(2) **Controlled work spaces.** If the work area is accessible only to persons who are authorized access to the SUI, additional protective measures are not needed. Again, the sub-team office must control the keys to the locks for these controlled work spaces.

c. At Home or On Travel. Working on SUI outside the workplace poses additional security risks and challenges. If there is a need to work with SUI at home or while on travel, the system manager's approval to do so must be obtained. Each individual holder of SUI is responsible for protecting it from unauthorized disclosure while at home or traveling. Whether working and storing SUI from home or an assigned travel destination, the information is to be provided the same level of protection that it is afforded at the normal work site.

9. DISTRIBUTION PROCEDURES FOR SUI

SUI may be carried, mailed, or shipped it in any manner that prevents inadvertent disclosure of the contents. When sending SUI records outside the DOT, include supplementary markings and notices to explain the significance of the information and promote its proper handling. For example, include a statement such as the following in a transmittal record or directly on the record containing SUI:

This document/record belongs to the Federal Aviation Administration and may be used for official government purposes only. It may not be released without the express permission of the Federal Aviation Administration. Refer requests for the document to:

(insert name and address of originating office.)

a. Hand carrying. Place the information in an opaque envelope or carry it within a brief case, pad folio, or other container. For FOUO information, use DOT Form 1600.7-1, FOUO Cover Sheet, or the FAA Form 1360-39, FOUO Envelope, if available.

b. Interoffice mail. Use a sealed opaque envelope with the addressee indicated on it. This is in addition to or instead of any office messenger envelopes. If available, use FAA Form 1360-39.

c. U.S. or Contract Mail. Mail or send documents and materials in properly addressed opaque envelopes or containers by United States Postal Service first-class, certified, or registered mail or contracted delivery service. Bulk shipments, such as directives, may be sent by 'fourth-class' mail provided the shipment is wrapped in opaque covering.

d. Telephone. Confirm that you are speaking to an authorized person before discussing the information, and inform the person that your discussion will include SUI and what part of the discussion is sensitive. Never leave voicemail messages containing SUI.

e. Fax.

(1) **Mark the fax.** Ensure that the documents being faxed are appropriately marked;

(2) **Send to correct number.** Use special care to ensure that documents are being sent to the correct fax number; and

(3) **Determine how faxes are handled at the receiving end:**

(a) If sending the fax to a controlled area, where only authorized persons will have access to it, then it may be sent without further precautions.

(b) If sending the fax to an uncontrolled area, where unauthorized persons might have access to it, then request an authorized person stand by at the receiving end while the fax is being sent. Ask for a confirming receipt.

f. **Electronic Mail.** Mark emails in the subject line “For Official Use Only” or “Sensitive Security Information” as appropriate. Send sensitive unclassified information as attachments; ensure they are appropriately marked IAW Appendices D and E of Order 1600.75. Also the security and encryption procedures of FAA Order 1370.81 must be followed.

g. **Web Sites.** Posting SUI to an unsecured web site that can be accessed by the public from the Internet is prohibited. Public web sites must not be provided links to web sites where SUI is posted. SUI may be posted to restricted FAA web sites provided they have special logon protocols and password protection. Passwords to these sites may be provided only to persons who satisfy the “duty to protect” and “need-to-know” requirements explained in Order 1600.75, chapter 2.

10. DISPOSAL OF SUI

The following guidance is provided for paper documents and record IAW requirements stated in Order 1600.75. Refer to the current version of this order to ensure this information is current.

Destruction Standards for Paper Documents and Records		
If your document is:	Then your destruction standard is	Method
FOUO	To make recognition and reconstruction difficult	At a minimum, tearing or shredding each page into small pieces and mixing those pieces into regular trash
SSI	Completely to preclude recognition or reconstruction	Burning, shredding, wet-pulping and chemical decomposition (Note 1)
SHSI	By any means approved for destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information	Burning, cross-cut shredding, wet-pulping and chemical decomposition
Destruction Standards for Paper Documents and Records		
If your document is:	Then your destruction standard is	Method
PCII	By any method that prevents unauthorized retrieval	Burning, cross-cut shredding, wet-pulping and chemical decomposition
Note 1: Existing strip shredders may be used, but cross-cut shredding is preferred. Any new shredding equipment must have a cross-cut feature. The local Servicing Security Element (SSE) can provide assistance in selecting an appropriate destruction method and equipment.		

Refer to appendix 4 for guidance pertaining to electronic/computer storage media.

CASE FILE/ NAS CHANGE PROPOSAL										Page 1 of _____	
(PLEASE TYPE OR PRINT NEATLY)											
1. Case File Number				2. For CM Use		Case File Received Date		NCP Issuance Date		NCP Number	
3. Scope of Change <input type="checkbox"/> Local <input type="checkbox"/> National <input type="checkbox"/> Test				4. Reason For Change <div style="display: flex; justify-content: space-between;"> <div> <input type="checkbox"/> Safety <input type="checkbox"/> Requirements Change <input type="checkbox"/> Baseline </div> <div> <input type="checkbox"/> Technical Upgrade <input type="checkbox"/> Design Error <input type="checkbox"/> Other </div> <div> <input type="checkbox"/> Systems Interface <input type="checkbox"/> Parts Unavailability </div> </div>							
5. Priority <input type="checkbox"/> Normal <input type="checkbox"/> Time-Critical <input type="checkbox"/> Urgent		6. Justification of Time Critical/Urgent Priority				7. Supplemental Change Form <input type="checkbox"/> ECR/ECP <input type="checkbox"/> TES <input type="checkbox"/> N/A 7a. Supplemental Change No. _____ 7b. Supplemental Change Initiation Date _____					
8. Case File Originator				9. Originator's Organization			10. Telephone Number			11. Case File Initiation Date	
12. Type of Document Affected <input type="checkbox"/> CPFS <input type="checkbox"/> SPEC <input type="checkbox"/> MTBK <input type="checkbox"/> _____ <input type="checkbox"/> TI <input type="checkbox"/> DWG <input type="checkbox"/> IRD/ICD								13. Baseline Document Number(s)			
14. CI Subsystem Designator				15. FA Type				16. CI Component Designator			
17. Facility Identifier (FACID)			18. Facility Code (FACCODE)			19. Cost Center Code			20. Software System Version		
21. Title											
22. Description: (a) identification of problem, (b) proposed change, (c) interface impact, (d) cost estimate (e) funding source (f) benefits/risks, (g) Schedule (h) Other (e.g. logistics, quality, etc.) <div style="display: flex;"> <div style="width: 50px; text-align: right;">(a)</div> <div></div> </div> <div style="display: flex;"> <div style="width: 50px; text-align: right;">(b)</div> <div></div> </div> <div style="display: flex;"> <div style="width: 50px; text-align: right;">(c)</div> <div></div> </div> <div style="display: flex;"> <div style="width: 50px; text-align: right;">(d)</div> <div></div> </div> <div style="display: flex;"> <div style="width: 50px; text-align: right;">(e)</div> <div></div> </div> <div style="display: flex;"> <div style="width: 50px; text-align: right;">(f)</div> <div></div> </div> <div style="display: flex;"> <div style="width: 50px; text-align: right;">(g)</div> <div></div> </div> <div style="display: flex;"> <div style="width: 50px; text-align: right;">(h)</div> <div></div> </div>											
Blocks 1 through 22 are to be completed by originator and/or the NCP coordinator. If a block is not applicable, write n/a. Attach additional sheets if necessary. See current revision of NAS-MD-001 for detailed completion instructions.											

Case File Number					NCP Number					Page 2 of ____	
23. Name and Title of Originator's Immediate Supervisor (Type/Print Clearly)					Signature					Date	
24. Facility/SMO Review (AT/AF)					25. Regional Review						
Name	Routing Symbol	Date	Concur	Non-Concur	Name	Routing Symbol	Date	Concur	Non-Concur		
					<input type="checkbox"/> Recommend Approval <input type="checkbox"/> Disapprove <small>(Enter into CM/STAT. Forward to Prescreening) (Return to Originator)</small>						
Routing Symbol	Signature				Routing Symbol	Signature					
Date					Date						
Routing Symbol	Signature				Routing Symbol	Signature					
Date					Date						
24a. Comments					Routing Symbol	Signature/Configuration Mgr/NCP Coordinator/ Reg Exec Sec					
					Date						
					25a. Comments						
(Attach additional sheets if necessary)					(Attach additional sheets if necessary)						
26. PRESCREENING											
Prescreening Office _____ Prescreening Comments: (Attach additional sheets if necessary)											
Reviewers	Routing Symbol	Date	Concur	Non-Concur	<input type="checkbox"/> Recommend Approval <input type="checkbox"/> Recommend Disapproval <input type="checkbox"/> New Requirement <small>(Return original to originating office through the Regional NCP Coordinator)</small>						
Recommended Must Evaluators					Routing Symbol	Signature					
					Date						
27. For Internal Configuration Management Use Only											

RECORD OF CHANGES

DIRECTIVE NO.

JO 6130.3A

[illegible]

