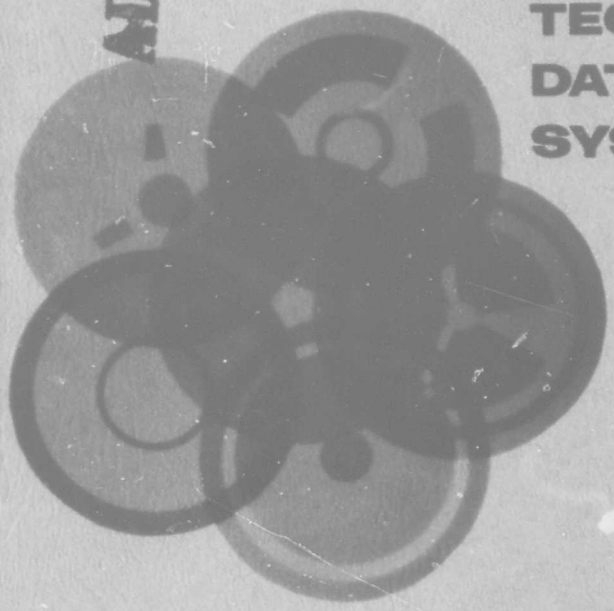
06349-W526-R0-00

INTEGRATED TECHNICAL DATA SYSTEM



DATA OPERATIONS SUBSYSTEM:

ADMINISTRATIVE MANUAL

JUNE 1969

PREPARED FOR

U.S. ARMY MATERIEL COMMAND

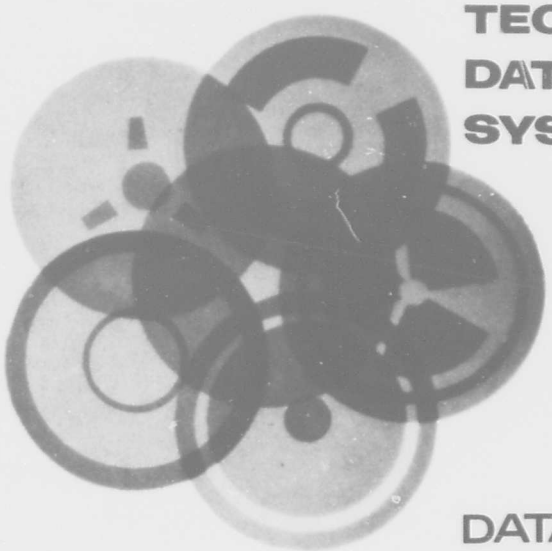
CONTRACT NO. DA-49-186-AMC-324 (X)

TRW SYSTEMS GROUP
WASHINGTON OPERATIONS
1735 I STREET N.W. • WASHINGTON D.C. 20006

SET I

06349-W526-R0-00

INTEGRATED TECHNICAL DATA SYSTEM



DATA OPERATIONS SUBSYSTEM:

ADMINISTRATIVE MANUAL

JUNE 1969

PREPARED FOR

U.S. ARMY MATERIEL COMMAND

CONTRACT NO. DA-49-186-AMC-324 (X)

TRW SYSTEMS GROUP

WASHINGTON OPERATIONS

1735 I STREET N.W. • WASHINGTON D.C. 20006

FOREWORD

TRW Systems was awarded a contract [Contract Number DA-49-186-AMC-324(X)] by the U. S. Army Materiel Command to develop an Integrated Technical Data System (ITDS). The ITDS is intended to provide assistance to the Army Systems Manager in performing his management and technical tasks by operating on relevant data to produce, summarize, and condense information. This allows the manager and technical support personnel to (a) determine status and monitor technical progress, (b) identify and predict system technical/management problems and their impact, (c) comprehend and evaluate proposed system changes, and (d) assign and maintain awareness of responsibility for action.

The ITDS is composed of personnel, procedures, equipment and computer programs. The organization of these elements provides a capability for the processing of systems program data, including the following functions:

- Data receipt and indexing
- Validation and verification for authenticy
- Storage
- Manipulation
- Retrieval
- Display and dissemination

The organization is divided into three major subsystems: the Functional Disciplines Subsystem, the Data Operations Subsystem, and the Computer Subsystem. ITDS user documentation, of which this manual is a part, is oriented to the above subsystems, with the exception of an overall System User's Guide and a Configuration Management Plan.

Following is a tabulation of ITDS user documentation (title of this volume is heavily underscored).

ITDS - overall:

- System User's Guide
- Configuration Management Plan

Functional Disciplines Subsystem:

- Administrative Manual
- Operations Manual
- Personnel Position Descriptions

Data Operations Subsystem:

- Administrative Manual
- Operations Manual
- Equipment Descriptions
- Personnel Position Descriptions

Computer Subsystem:

These 12 manuals, in general, cover administration of the subsystem, operating and maintenance instructions for the programs, computing equipment descriptions, and personnel position descriptions.

- Administrative Manual
- Generalized Processing Program, General Description
- Applications Programs, General Descriptions
- Peripheral Programs, General Descriptions
- Computer Programs Maintenance Manual
- Computer Programs Operations Manual
- Data Processing Center Operator's Manual
- Equipment Descriptions
- Personnel Position Descriptions
- Generalized Processing Program, Programming Documentation
- Applications Programs, Programming Documentation
- Peripheral Programs, Programming Documentation

This manual describes administrative policies, procedures and control methods used by the Data Operations Subsystem. References are made to other ITDS documents for more details about some of the subjects introduced herein.

CONTENTS

CONTENTS (Continued)

ILLUSTRATIONS

DATA OPERATIONS SUBSYSTEM: ADMINISTRATIVE MANUAL

1. INTRODUCTION

1.1 PURPOSE

This manual is intended as a ready reference for the user of ITDS data operations services. It is also intended to assist ITDS personnel in the manual processes of acquisition, control, analysis, storage, and retrieval of project documents and data.

1.2 SCOPE

This manual serves as a companion to ITDS Data Operations Subsystem: Operations Manual, which prescribes operational procedures for the Data Operations Subsystem. This manual supplements the operational manual with the following:

- Instructions for compliance with procedures for the protection of classified information, including approved methods for receipt, custody, storage, and issue of classified documents and data.
- Examples and brief instructions for use of typical administrative forms used with the ITDS to control and record the distribution, storage, and updating of documents and digital data.
- Examples of reference materials used in determining responsibilities for processing incoming documents for action, information, data extraction, and/or for decisions to dispose of documents that are not needed for future reference.

1.3 GENERAL

Data operations work procedures and task sequences can be varied greatly, depending on how ITDS is applied. In any application, however, certain administrative policies remain constant to assure compliance with directives from senior authorities and to ensure high-quality ITDS services at economical operating costs. These ongoing administrative policies are summarized below.

1.3.1 Compliance with Administrative Directives

Military offices are subject to administrative directives issued by higher authorities. ITDS data operations will be conducted in compliance with such directives. Higher level administrative directives are particularly germane to the following data operations activities:

- Protection of classified information.
- Maintenance, storage, and disposal of official Army records.
- Preparation, authentication, and submission of prescribed recurring reports.
- Participation in directed programs for the management and control of administrative forms. The obligation is inherent to make use of existing forms whenever practicable.
- Compliance with established procedures for correspondence control and management.

1.3.2 Production Control

For ITDS users who do not have direct electrical input/output access to the digital data base, the Data Operations Subsystem will provide production control services for documents enroute between the users and the Computer Subsystem. Production control will include identifying, receipting, and batching data submittal forms and computer products. Documents will normally be processed on a "first in, first out" basis. When it is necessary, however, priorities will be assigned on the basis of software dependencies or upon requirements of output products.

Production control will receive and account for computer hard copy products and deliver them to product users and requesters.

Production control records will be manually posted and maintained with sufficient detail to identify all work-in-process, points of origin and destination, transaction completion event dates, required schedules, and priorities.

1.3.3 Administrative Quality Control

All incoming ITDS documents and all internal documents that pass through the production control activity of data operations will be inspected for administrative adequacy. Actions will be taken to correct significant deficiencies of legibility, format, completeness, identification, source indication, or numbers of copies. The highest quality requirement will be assigned to documents that are to be distributed outside the system or program office. One-time deficiencies that do not degrade the communication of information can be accepted if justified by economy and timeliness. In such a case with a scheduled report, corrective action will apply to follow-on issues at the earliest practicable date.

2. SECURITY PROCEDURES

The Data Operations Subsystem adheres strictly to prescribed procedures for the control of classified or sensitive documents and information from the time of receipt until proper disposition. Those procedures cover accounting, physical security, and access control. The procedures involve additional steps, not shown on the function flow charts of this series, which are numerous and which depend upon the security classification of the data.

The design of ITDS is appropriate for a variety of environments, and the security procedures must satisfy the requirements of the organization within which it is installed. Assuming that ITDS is being operated by Army personnel in support of a Manager in the Army Materiel Command, the security procedures are defined in the 380 series of U. S. Army regulations, by the 380 series of AMC regulations and by AMC memorandums.

Classified data are kept on separate memory banks to avoid the possibility of compromise. Access to classified computer data is limited by the access procedures of paragraph 7 as well as this paragraph. If any memory device or any data of a classified nature is accessible by the computer then the entire computer system, and access to it, must be treated according to the rules pertaining to the highest classification of data accessible.

2.1 SPECIAL PROBLEMS

ITDS poses special problems if security data are to be processed by the computer. AR 380-46 explains the restrictions on the use of information processing equipment with classified data. Electronic transmission of classified information on commercial telephone lines is prohibited unless encryption is practiced under rigid control.

2.2 NORMAL INFORMATION FLOW CONTROL

The design of ITDS provides for control and accountability of all documents, even though they may be unclassified. For this reason, when ITDS is operated in an administrative environment which permits it, the ITDS administrative procedures can control classified information within the normal routine. These procedures can be modified to conform with the security practices of the host organization.

2.3 SECURITY OF CONTROL FILES

The administration of data flow in ITDS results in several suspense files and several logs of control numbers being operated. These files and logs are not classified security data in the strict sense of the term; however, they are extremely important to the operation of ITDS. The system would have no way to guarantee efficiency and responsiveness without them. Therefore, it is necessary to provide an effective level of protection from accidental or deliberate damage, loss, or tampering. All such files and logs will be kept locked up when not under surveillance by personnel responsible for their use. Backup personnel must be assigned, trained, and tested so that absence of persons with primary responsibility will not jeopardize system operation.

3. DATE AND TIME STAMP PROCEDURES

All data, in whatever format, which is received by ITDS must have the date and time of receipt clearly stamped or affixed. This must be done prior to any type of document review or format conversion. This facilitates the subsequent monitoring of document progress and the determination of processing priorities. The clerk who receives the "mail" or input data applies the stamp uniformly to valuable and nonvaluable documents, without regard to content, before he takes any other action.

4. INITIAL REVIEW AND ROUTING OF INPUT DOCUMENTS

A senior data analyst who is familiar with the ITDS will perform the initial review of incoming data, will make appropriate decisions with regard to applicability, and will mark the desired routing for each document.

4.1 DISTRIBUTION TABLES

The analyst will maintain and use a set of tables, similar to Fig. 4-1, which will indicate by document category or title the office(s) which are to receive copies of each document by type. This set of tables will be amended frequently so as to be constantly current. The tables will show details such as the following:

- office of primary interest (OPR) if applicable;
- action office, if applicable;
- office(s) of information interest, or secondary interest;
- titles of all recurring incoming reports;
- number of copies, if applicable, going to each office.

4.2 DISTRIBUTION AND COORDINATION FORM

The analyst will use a stamp or will attach a form, similar to Fig. 4-2 to the action copy of each document, with appropriate notation to indicate its subsequent routing.

4.3 DOCUMENT IDENTIFICATION NUMBER

The analyst will assign to each document which is to be retained in the system a unique identifying number (referred to as the "ident" or the "DAI" number). This number will be entered on the original and all copies of each document prior to the reproduction of additional copies. The number must be entered on the distribution form; if it is a separate sheet rather than a stamp, this form becomes a permanent record in addition to the original or action copy. The number is extremely important because it is the key to all indexing and library functions. Therefore, the analyst controls the assignment of these numbers with utmost discipline to assure that different documents never have the same number and that all numbers in sequence are accounted for.

ACTION ITEM RESPONSIBILITY CHECKLIST

PAGE_____

DATE_____

DIVISION/OFFICES/ ACTIVITIES	PM	PS	TM	CM	PA	PB	SA	FO	FO	FO	KO	LEGEND
SUPPORT DIVISION												
Business Information (NOI)	A	P										A Approval required (correspondence pertaining to cost, schedule, and/or contracts)
Contractor Data Requirements List	A	P	C	C*	C	C	C	S	S	I		C Coordination required
Correspondence, PMO Admin (NOI)	A	P										I Information office and/or ITDS entry
Data Submittals, Contractor	A	P	P	P	P	P	P	P	P			NOI Not otherwise identified
Integrated Technical Data System (ITDS) Contract & Information	A	P	I	I	I	C		I	I	I		P Primary responsibility
News Releases	A	P	C	C								S Secondary action or support required
Personnel Action (NOI)	A	P	C*	C*	C*	C*	C*	S*	S*	S*		* As required
Regulations (Subject)	I*	P	S*	S*	S*	S*	S*	S*	S*	S*		
Security	A	P	S	S	S	S		S	S	I		
Prime Contractor GFM Data	A	P	C	C	C		C	S	S	I		

Figure 4-1. Sample Action Item Responsibility Checklist

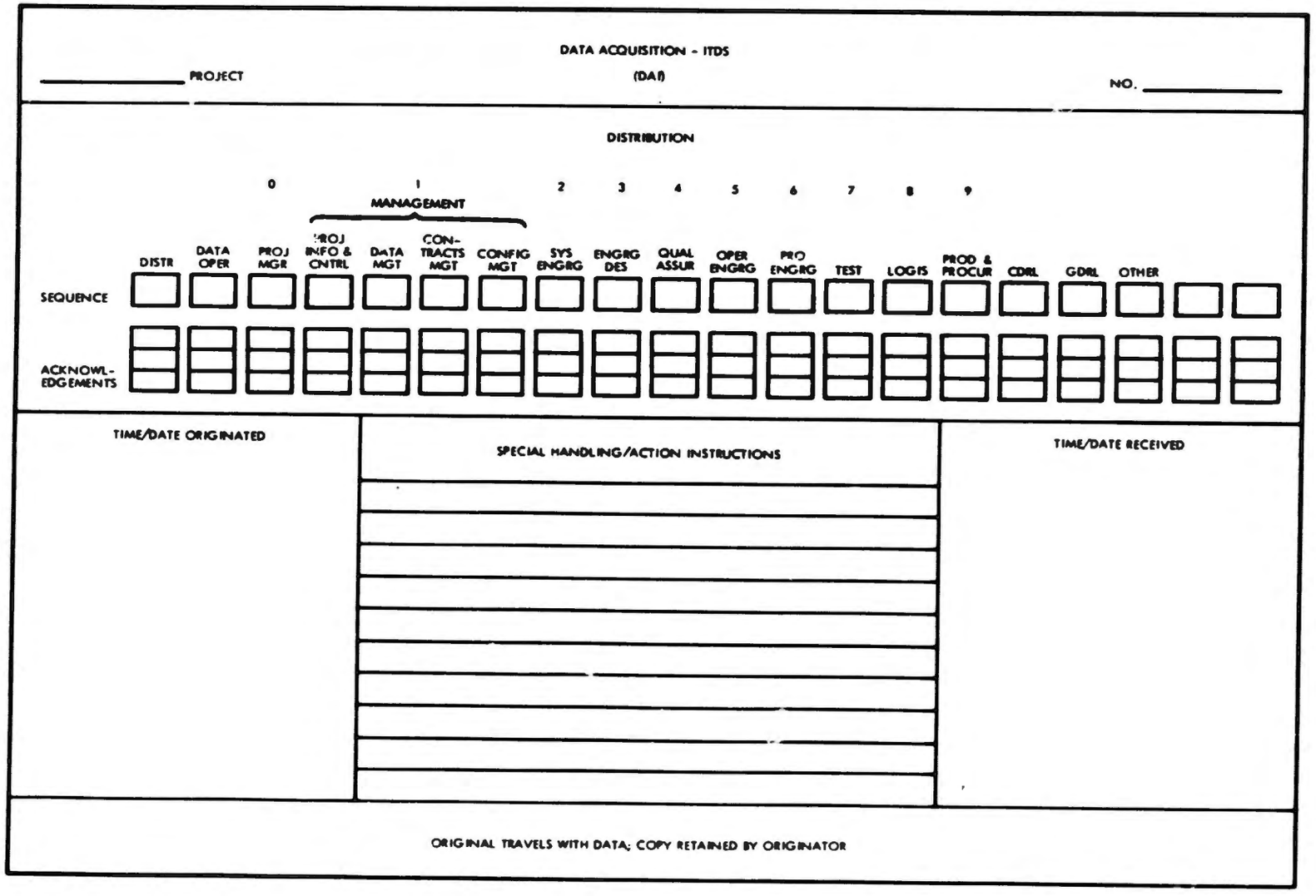


Figure 4-2. Sample Data Acquisition Form

4.4 SPECIAL HANDLING INSTRUCTIONS

Some documents require special actions or handling, and the analyst will prescribe these in the place provided on the form. He will indicate the offices to which extra copies are to be sent. The normal policy and routine will be to provide copies to several offices simultaneously whenever it appears that this might expedite system response. The reproduction distribution clerk will make additional copies to satisfy the expanded distribution.

4.5 INQUIRY CONTROL NUMBER

The analyst will identify as inquiries those documents which require system output as distinguished from the many documents which are only input to the data base. He will assign an inquiry control number to each of these documents in addition to the regular document identification. The inquiry control number serves as a flag which calls attention of the OPR to the need for prompt attention to the document. The control log listing of inquiry control numbers is delivered daily to the inquiry control desk; the log is used to assure that all inquiries are responded to expeditiously.

4.6 ACTION ITEM DESIGNATOR (AID)

The analyst will identify the documents which will be monitored with the Action Item System. He will use a reference matrix similar to that of Figure 4-3 and will follow procedures as explained in the Action Item System documentation.

4.7 VOIDING A DOCUMENT IDENTIFICATION NUMBER

A form such as that in Figure 4-4 will be used whenever it becomes necessary to void an identification number. Sometimes two copies of the same document arrive at different times at the input station. Occasionally documents are accepted initially as system inputs which subsequent processing steps reveal to be irrelevant. These and other problems can make it appropriate to void a control number. Voiding slips must be processed so as to update both the hard-copy library and digital data base. Various persons may originate voiding slips, beginning with the data analyst who accomplishes initial input processing; the person who discovers the error has the basic responsibility to initiate corrective action.

ACTION ITEM RESPONSIBILITY CHECKLIST

Page_____

Date_____

DIVISION/OFFICE ACTIVITIES	PM	PS	TM	CM	PA	PB	SA	FO	FO	FO	KO
CONFIGURATION MANAGEMENT OFFICE											
Configuration Management/Accounting	A	1	S	P	C	C	I	C	C	I	
Description Change Proposal (DCP)											
Airframe	A	I	S	P	I	C		S	I	S	
Armament	A	I	S	P	I		S	I	I	I	
Avionics	A	I	S	P	I		I	I	S	I	
Engine	A	I	S	P	I			S	I	I	
Fire Control	A	I	S	P	I		S*	I	S	I	
Ground Support Equipment (GSE)	A	I	S	P	I		S*	S	S*	I	
Design Baselines											
Airframe	A	I	S	P	I			S	I	S	
Armament	A	I	S	P	I		S	I	I	I	

LEGEND

- A Approval required (correspondence pertaining to cost, schedule, and/or contracts)
- C Coordination required
- I Information office and/or ITDS entry
- NOI Not otherwise identified
- P Primary responsibility
- S Secondary action or support required
- * As required

Figure 4-3. Sample Action Item

ITDS DOCUMENT VOID REQUEST

DAI NO. (S) _____ SUB DAI NO. (S) _____ PROJECT _____

REASON FOR VOIDING DOCUMENT

DUPLICATE ☐ ☐ INAPPLICABLE ☐ DMO DIRECTION

DISTRIBUTION FOR "INAPPLICABLE" DOCUMENTS

DEPARTMENT	(INITIAL)	CONCURRENCE	NON CONCURRENCE

VOID ACTION COMPLETED

(INITIAL)

DATA ANALYSIS _____

DATA CONTROL _____

DMO SUPPORT SECTION _____

NAME OF ORIGINATOR _____ DATE _____

Figure 4-4. Sample Document Void Request

5. DATA BANK INQUIRY FORM

This form, Figure 5-1, is provided to expedite retrievals which originate within ITDS. It is important to remember that inquiries can be originated in three ways: 1) by direct access using an inquiry terminal, 2) by submitting a document to ITDS from an external source, and 3) by submitting this Data Bank Inquiry form if the originator is within ITDS. The documents which are submitted to ITDS from an external source, and which are inquiries, are processed and sent to the OPR, which may in turn originate an "internal" request by using this form.

5.1 USING THE FORM

The OPR for the inquiry being processd, if unable to satisfy the request by direct access, will prepare the form and submit it to the Data Operations Subsystem for action. If the request is for computer processing the Input-Output Control Desk of the Data Operations Subsystem will accomplish necessary checking, priority queuing, and control, and will submit it to the Computer Subsystem. If the request is for simple hard-copy retrieval, the request is submitted to the library. The LOG NUMBER at the upper left corner is the same as the Inquiry Control Number mentioned in paragraph 4.5. The OPR must fill out the SUBJECT and DESCRIPTION in precise detail, preferably in correct access language, so that the retrieval can be made without further study. The overall purpose of this form is that of a worksheet, remaining in action until the requested information is returned to the in-house requester, the OPR.

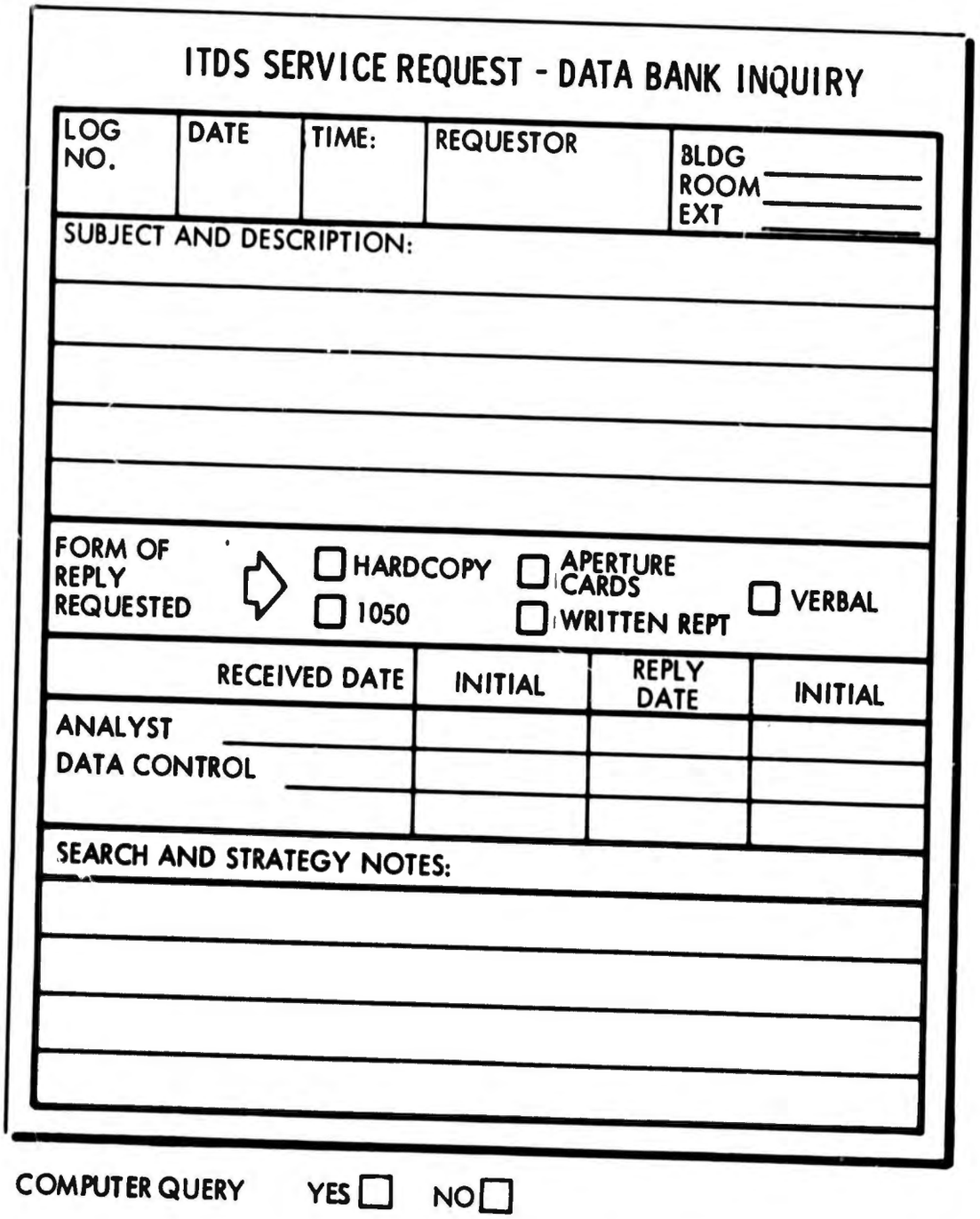


Figure 5-1. Sample Data Bank Inquiry

6. USER SERVICE REQUEST

Figure 6-1 illustrates a typical input control slip of the kind that must be used for submitting work to the Computer Subsystem for processing. It is to be expected that some implementations of ITDS will rely on computer installations that have many responsibilities other than ITDS, and strict control over the interface between the Data Operations and Computer Subsystems will expedite the orderly flow of work. As a general rule, jobs which change the contents of data lists must be authorized by the proper Data Operations Subsystem signature before the Computer Subsystem accepts them for processing. Data Operations Subsystem must make sure that the OPR has the authority and has signed the form before processing the job. See Section 7 for further details about access authority.

6.1 COPIES OF USER SERVICE REQUEST

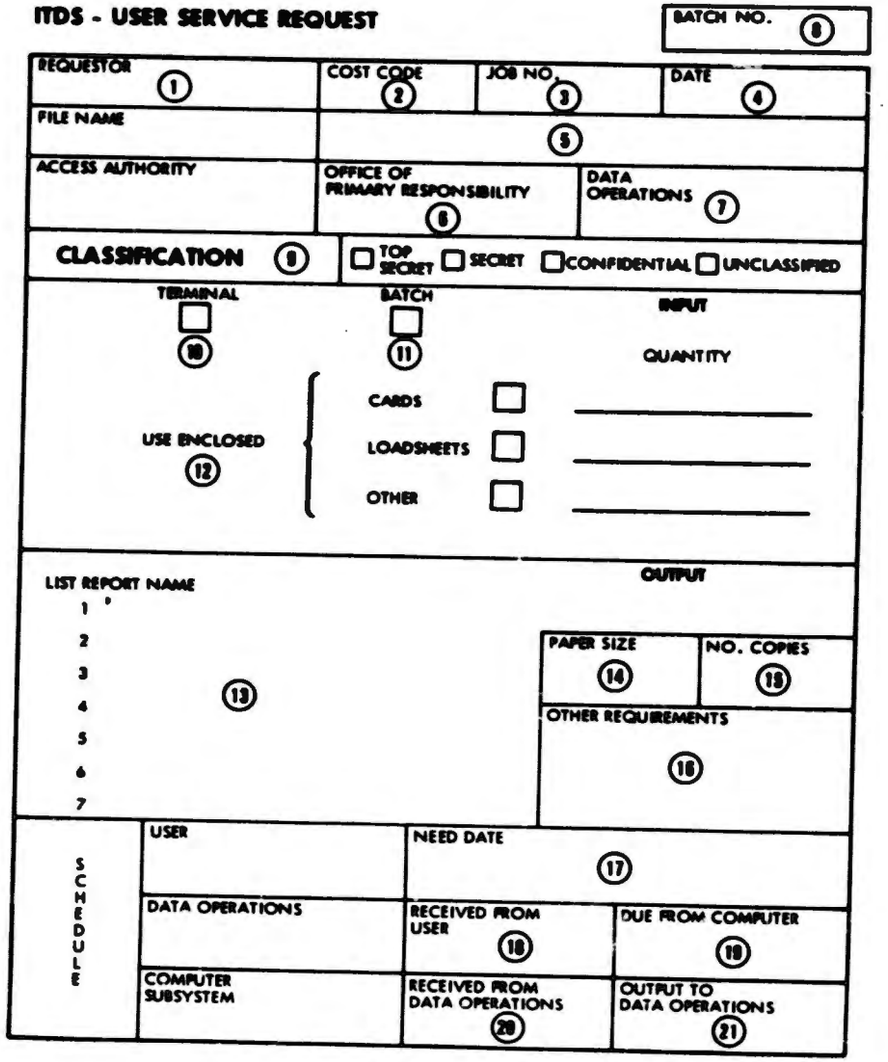
The form will be manufactured so as to provide four copies, already attached together and treated with copying chemicals to act as "automatic carbon paper." The top copy will travel with the job. The fourth copy (bottom) will be retained by the originator. The third sheet will be held in suspense by Data Operation Subsystem after submittal of the job to the Computer Subsystem until the completed job is returned by Computer Subsystem to Data Operation Subsystem; Data Operation Subsystem will mark the third copy with the date/time received from Computer Subsystem and will retain the third copy for 90 days for statistical use. The second sheet will be retained by Computer Subsystem.

6.2 BATCH NUMBER

The batch number is assigned by the person who is operating the Input-Output Control Desk within Data Operation Subsystem. This number is derived from and controlled by means of a log-book maintained by the Input-Output Control Desk. The log-book is a permanent system record.

6.3 PROCESSING INSTRUCTIONS

The User Service Request has very little space for writing special instructions. It is primarily for acctounting purposes. It must be supplemented in some cases with instruction sheets to explain the necessary details



INSTRUCTIONS FOR PREPARATION OF USER SERVICE REQUEST

(1) NAME OF THE PERSON REQUESTING COMPUTER SERVICE.

(2) COST COLLECTION NUMBER, IF APPLICABLE.

(3) THE SPECIFIC JOB NUMBER OF THE REQUESTOR, WHICH IS AN EXTENSION OF THE COST COLLECTION ACCOUNT RECORDED IN (2). THIS IS THE COST ACCOUNT AGAINST WHICH THE COMPUTER SERVICE IS TO BE CHARGED.

(4) DATE THE USER SERVICE REQUEST IS PREPARED.

(5) NAME OF THE DATA FILE(S) AFFECTED.

(6) AUTHORIZED SIGNATURE FROM THE OFFICE OF PRIMARY RESPONSIBILITY FOR ACCESS TO THE DATA BASE.

(7) AUTHORIZED SIGNATURE FROM DATA OPERATIONS VERIFYING ACCESS.

(8) BATCH NUMBER ASSIGNED BY DATA OPERATIONS.

(9) SECURITY CLASSIFICATION – CHECK THE APPROPRIATE BLOCK.

(10) TERMINAL ACCESS – CHECK IF REQUEST IS FOR DIRECT ACCESS TO THE DATA BASE.

(11) BATCH – CHECK IF FOR OTHER THAN DIRECT ACCESS TO THE DATA BASE.

(12) INDICATE TYPE AND QUANTITY OF INPUT CARDS OR LOADSHEETS.

(13) LIST THE DESIRED OUTPUT REPORTS BY NAME.

(14) PAPER SIZE OF THE DESIRED OUTPUT.

(15) NUMBER OF COPIES OF THE DESIRED OUTPUT

(16) OTHER REQUIREMENTS

(17) USER NEED DATE.

(18) DATA OPERATIONS ENTRY.

(19) DATA OPERATIONS ENTRY.

(20) COMPUTER SUBSYSTEM ENTRY.

(21) COMPUTER SUBSYSTEM ENTRY.

Figure 6-1. ITDS - User Service Request

of the job to the Computer Subsystem. For simple inquiries, the Data Bank Inquiry sheet (see Section 5) will often suffice. For complex processing jobs which involve many steps, the OPR which originated the job must provide detailed written instructions in addition to the Input Control Slip.

6.4 ACCOUNT NUMBER

The OPR or the Input-Output Control Desk will assure that the proper cost account code is recorded after COST CODE. This is for the purpose of billing computer time. The Data Operations Subsystem will issue an administrative directive in which the proper account numbers will be listed.

7. ACCESS TO DATA LISTS

ITDS provides conceptually for any degree of control that may be required to be exercised over access to system data. In the least controlled form, anyone at all would have authority to change or to query any data list. In the most controlled form each authorized user would have two access code numbers, one for updating and one for accessing data lists; each data list would allow update from only a specific list of authorized users; and each data list would allow queries from only a specific list authorized users.

In practice there are two levels of access control. Both of these levels of control are based upon the proprietary authority of the host or organization. The first level restricts the right to use the system to personnel of ITDS and such other persons as the host may name. An Army major might typically name just one or two individuals within his office to have access. The second level of access control limits the authority to change the data in a data list to the OPR for that data list, and it limits query access for a few specified files. Most files (data lists) are accessible for queries from all authorized users.

7.1 ACCESS PROCEDURES

Figure 7-1 shows the actions, or responsibilities, of the four different categories of people who are primarily involved in access control. The ensuing paragraphs discuss briefly the five listed actions.

7.2 PUBLISH ADMINISTRATIVE DIRECTIVE

The Data Base Management Office (DBMO) of the Data Operations Subsystem is responsible for controlling access to the data base. Its most basic act in fulfilling this responsibility is to coordinate, publish, and and maintain an administrative directive which will establish both general guidance and detailed procedures. This directive must be approved by the proprietary authority and must be coordinated with the Computer Subsystem and the Functional Disciplines Subsystem, including the most important OPR's, prior to publication. From time to time, as it becomes apparent that changes in the directive are needed, the DBMO will initiate the changes by redrafting the directive and reiterating the publication procedure. The

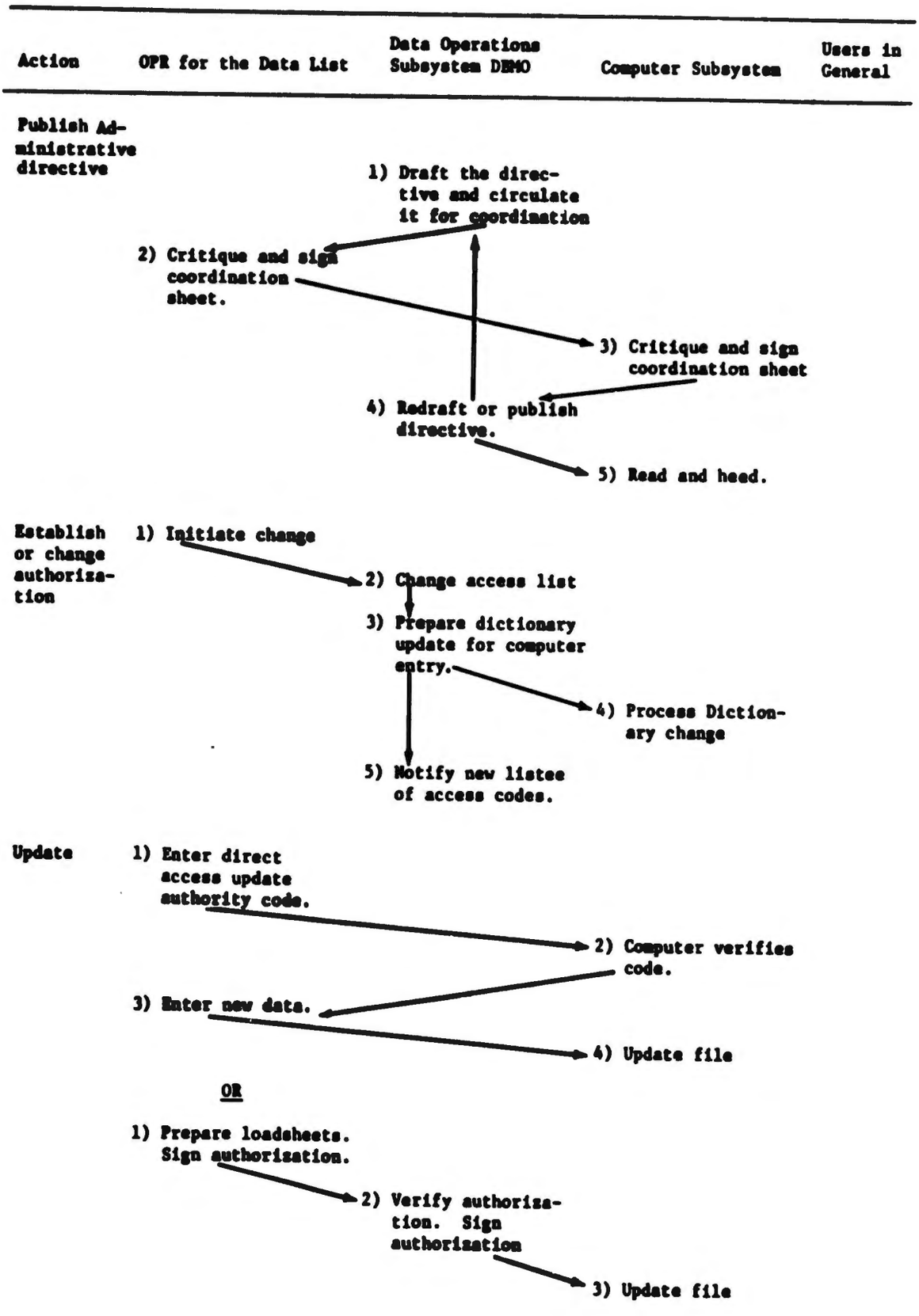


Figure 7-1. Access to Data Lists, Authorization, and Control

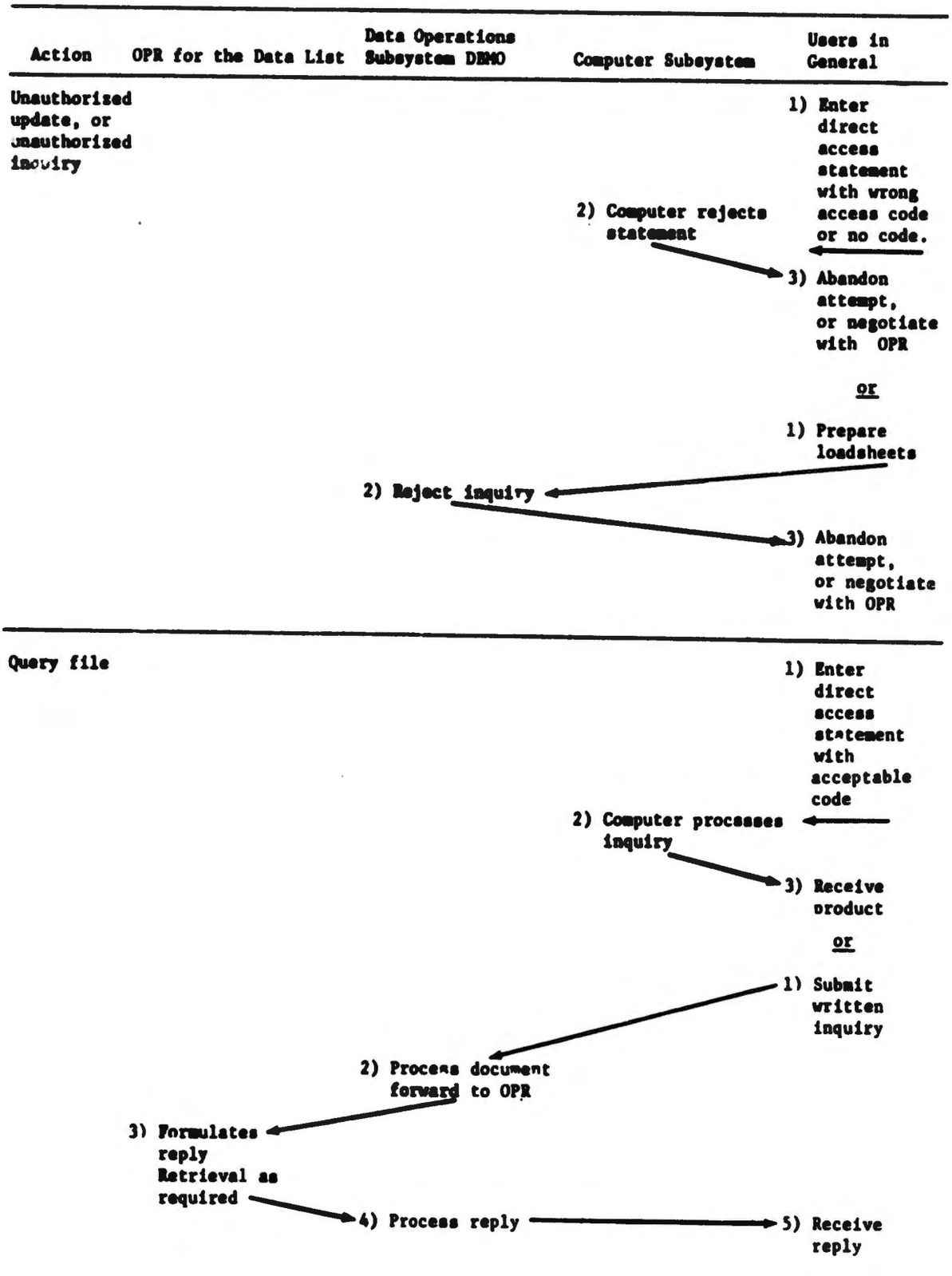


Figure 7-1. Access to Data Lists, Authorization, and Control (Continued)

procedure for assigning the OPR will vary somewhat on different projects, and will be published by the on-site system manager.

7.3 ESTABLISH OR CHANGE ACCESS AUTHORIZATION

The OPR for each data list is responsible for establishing any needed restrictions on the data list. The OPR will provide the DBMO a written request, giving necessary details. The DBMO will accomplish the change, including modification of master access lists, assignment of access code (if applicable), updating of computer dictionaries, submission of input to the Computer Subsystem, and notification of concerned persons, if appropriate, that the action is complete.

7.4 UPDATE FILE

Normally it will be the responsibility of the OPR to update its own data lists, and all other parties will be prohibited from doing so. Most files will be protected with update access codes known only to the OPR's and the DBMO. The OPR will prepare the data, the input control slip, and any necessary special instructions, and give the package to the Input-Output Control Desk of the DBMO. This procedure will require the inclusion of the access code as the first statement processed. Also, the OPR must include the proper signature on the form. The Input-Output Control Desk verifies the access authorization and processes the package. Alternatively, the OPR may update its data list by direct access if the computer verifies the code that is entered.

For discussion purposes, it is convenient to think of updates being authorized, or initiated, only by the OPR for the data list. If the OPR chooses to allow non-OPR people to know the update code, the ITDS will react as though these people were authorized members of the OPR.

7.5 ATTEMPTED ACCESS

If an unauthorized person attempts to update or query a file using an improper code, ITDS will reject the attempt, whether it is made by direct terminal communication procedures or by submission of documents. The unauthorized person must either negotiate with the OPR to obtain permission or abandon the attempt.

7.6 NORMAL ACCESS FOR INQUIRIES

Most files will be freely accessible, for inquiries, to the people who are authorized to use ITDS. Such files will not require any access code for retrieval of information. Processing of such inquiries is done without questioning the authorized inquirer.

There will be, in most ITDS applications, some files which few people may query. These data lists will return the requested information only to requesters with proper authority.

Inquiry processing is discussed in Section 5.

8. INCIDENT REPORTING SYSTEM

An incident reporting system will be established for the purpose of recording all significant error messages and complaints, and for monitoring follow-up action. The DBMO will exercise administrative control over this system, publish the required directives and forms, record the reports, and assign responsibilities for taking corrective actions. The incidents will include all categories of computer-generated error messages and also all system anomalies or defects which are reported by humans.

8.1 INCIDENT REPORT FORM

Figure 8-1 is a typical form that might be used. The main problem in reporting incidents is that of including sufficient information to enable the trouble-shooting personnel to accurately duplicate, observe, and correct the deficiency. Thus, the form includes words, blanks, etc., which prompt the respondent to give a thorough description, even though he might not fill in every blank space. An incident report must be filed for every incident that is not cleared up by prompt and informal coordination.

8.2 SUMMARY OF INCIDENTS

The incident reporting system is one of the most effective tools available to the ITDS manager for maintaining and improving ITDS efficiency. Its importance cannot be over-emphasized. Hence, the DBMO must provide the ITDS manager a daily summary of newly-reported incidents, progress in correcting old incidents, and corrective actions terminated. The format of the daily summary report will be determined according to its size and local administrative procedure.

INCIDENT REPORT

Date/Time_____

File(s) involved_____

Was the computer involved?_____

If so: Was generalized access language involved?_____

If so, attach printout of statement or include verbatim in remarks below.

Was a peripheral program involved?_____

Which one?_____

Was an applications program involved?_____

Which one?_____

Was the defect caused by deficient administrative directives?_____

If so, explain_____

Was the deficiency caused by personnel errors?_____

If so, please be specific_____

Detailed narative: (Include all significant events and attach all printouts, or copies of other pertinent documents.)

_____

_____

_____

_____

Name, location, telephone no.:_____

_____

Figure 8-1. Typical Incident Report

9. KEYPUNCH ADMINISTRATIVE PROCEDURES

Keypunch personnel are often thought of as belonging to the Computer Subsystem. This arrangement can be varied, if circumstances warrant it, by placing some keypunch personnel (those who work on data flow) under the operational supervision of the Data Operation Subsystem. If this is the case, administrative practices must be devised accordingly. Specifically, quality control and job accountability practices must apply to the key-punch work. The quality control function will usually include a key-verifier capability and spot-sampling-checking by a supervisor. The job accountability function will have to include card-count and timeliness.