

## 3 GETTING STARTED

### 3.1 INTRODUCTION

Message switching simply defined is sending a message from one workstation location to another workstation at a different location. In order to accomplish the message switching through the computer, the information to be transmitted must be in a prescribed format. The message format is flexible and allows for the handling of original messages as well as additions or replies. Strict adherence to the standard formats will insure accuracy and minimize delay in message handling. There are eight different message types. However, the basic message format is the same for each type. An example of the different messages and construction is explained in this section. To determine if your workstation is communicating with LEADS and obtain the time of day, use the following format: TOD. (TRANSMIT)

Response: WEDS 2000/10/25 (Year, Month, Day)  
          07:00:00 (Time: Hours/Minutes/Seconds)  
          JULIAN 299 (Julian Calendar Date)

### 3.2 SENSITIVITY OF DATA

The LEADS continues to grow as criminal justice agencies elect to become active participants. There is more data stored each day and more inquiries into the files. As we continue to expand, we must continually be aware of the responsibility and liability associated with the data we contribute and the data we retrieve.

Data accessed through LEADS, NCIC, NLETS and other intra-state systems is restricted to the use of duly authorized law enforcement and/or criminal justice agencies and is not to be sold, transmitted or disseminated to any non-law enforcement agency, non-criminal justice agency or unauthorized person. *Participating agencies have assumed responsibility for system security and integrity when they execute the LEADS participation agreement (LEADS Administrative Rule 4501:2-10-13).*

LEADS terminal agencies can provide data received via LEADS to other criminal justice agencies. To be considered as a criminal justice agency they must have an Originating Agency Identifier (ORI) assigned.

#### 3.2.1 Audit Trail

When an inquiry is made into the system it is automatically recorded to a tape-log at LEADS Control and if the inquiry is sent to NCIC it will be tape-logged there also. The tape-log is the start of the audit trail. It can be searched later, upon request through the LEADS Security Office, to determine when and if an inquiry was made about a particular person, vehicle, article, etc. The LEADS tape-log is maintained for six years.

LEADS operators can also place the name, unit number, badge number or other identifier of the requestor for social security checks, operator's license checks, and registration checks after the inquiry format.

*Example:*

```
DS.123456789.OFFICER D SMITH(TRANSMIT)
RP.BMV0001,PC.UNIT 824(TRANSMIT)
```

When running inquiries for non-terminal agencies, you must include their ORI in the inquiry. Their ORI is placed after the initial inquiry type identifier, followed by a period, and then the remainder of the inquiry format as usual. The DS and RP inquiries can also include the requestor's name, unit number, etc.

*Example:*

```
DS.OHOHP0098.123456789.OFFICER D SMITH(TRANSMIT)
RP.OHOHP0098.BMV001,PC.660(TRANSMIT)
QW.OHOHP0098.NAM/PUBLIC,JOHN Q.DOB/121340.SEX/M(TRANSMIT)
QV.OHOHP0098.VIN/12AB34CD56EF78GH9(TRANSMIT)
```

When a computer printout is transmitted or disseminated to an authorized individual or criminal justice agency the participating agency should indicate on the computer printout:

1. to whom the printout will be given;
2. date and time stamped (or handwritten) to document when the printout was forwarded to the receiving individual, court, etc. The terminal ORI should be left intact on the printout and not removed or defaced so an audit trail is in place.

Faxing of LEADS printouts is permissible providing you are confident the person on the receiving end is criminal justice personnel and entitled to receive the information. Before faxing the printouts, they must be marked with an audit trail as defined above. In the case of CCH printouts, the receiving person must fax back a signed receipt.

### **3.3 OHIO LEADS AUDIT PROGRAM**

The foundation on which a criminal justice computer network is built is the ability of that network to provide to the criminal justice community complete, accurate, and timely information. There is a great concern today for the security and accuracy of data stored in criminal justice communications systems. The primary responsibility for the integrity of the data in these systems lies with the originating agency.

In 1985 the NCIC Advisory Policy Board mandated each state accessing NCIC files must have an audit program in place which would require all agencies accessing NCIC to be audited every two (2) years.

The purpose of an audit is to bring the data submitted into NCIC/LEADS files to a high level of quality and accuracy. To accomplish these ideals, we have entered into a program to evaluate LEADS/NCIC use within Ohio agencies.

### **3.3.1 Objectives**

The audit will have two basic objectives:

1. To provide reasonable assurance appropriate control systems have been established by the agency administrator to insure compliance with law and policy.
2. To provide reasonable assurance the terminal agency has instituted sufficient controls to guarantee their entries provide reliable and accurate information.

### **3.3.2 Areas Covered in the Audit**

1. Type and reasons for access to the "hot" files and III.
2. Disposition of information provided by the Control Terminal Agency (CTA) at the user level.
3. An examination of the quality assurance measures in effect.
4. Security.
5. Training.
6. Validations.

### **3.3.3 Methodology**

Biennial audits shall be conducted by members of the audit staff at each terminal agency which makes entries or inquiries into LEADS/NCIC files. The audit process will focus on improvement.

1. The Auditor will contact the agency to determine a mutually acceptable date and time to conduct the on-site audit. Correspondence confirming the arrangements will be sent to the agency.
2. Prior to the on-site audit the TAC will:
  - a) Reproduce and complete the pre-audit questionnaire contained in this section of this manual. (See Section 1.8 of the LEADS Operating Manual.)
  - b) Retrieve a list of certified operators from the LEADS workstation and make necessary corrections. (See Section 3.4 of the LEADS Operating Manual.)

The pre-audit questionnaire and the certified operators list will be maintained at the agency and reviewed during the on-site audit by the Audit Staff to determine compliance with all applicable Federal law, State law and policy requirements.

3. The Auditor will conduct an initial interview with representatives of the agency being audited. The interview will consist of:
  - a) Process
  - b) Purpose
  - c) Objectives
4. The on-site phase of the audit will consist of a review of agency practice to insure conformity with policy. The audit will include review of non-compliance with applicable laws, regulations, policies or procedures. If instances or indications of fraud, abuse or illegal acts are found during, or in connection with the audit, the Auditor will contact the Control Terminal Officer (CTO - Chairman of the LSC) at first indication for guidance. In addition, the on-site audit of the terminal agency will include quality assurance and other areas that can only be reviewed at the terminal agency, i.e., dissemination, validations, LEADS Newsletters and Manuals.
5. The Auditor, using the agency evaluation form and documentation previously prepared, will then audit selected records from those supplied. This comparison review will insure users are in compliance with the policies and procedures.
6. After completion of the on-site audit, the Auditor will meet with the agency administrator for an exit interview. The Auditor will review the agency evaluation and all findings. Recommendations will be made for actions to improve problem areas found during the audit and to improve operations. Pertinent views of officials of the organization audited concerning the Auditor's findings, conclusions and recommendations will be sought. When possible, these views should be obtained in writing. Any exceptions to the findings of the Auditor can be made by the terminal agency at this point.

7. A description of noteworthy accomplishments, policies and procedures is appropriate; particularly management accomplishments in areas which can be recommended to other agencies.
8. The Auditor will submit the completed agency evaluation form to the CTO. If the agency must follow-up with written correspondence advising specific actions taken to correct problem areas, the cover of the report shall note that requirement.

### 3.3.4 LEADS PRE-AUDIT QUESTIONNAIRE

Agency \_\_\_\_\_ ORI \_\_\_\_\_

Completed by \_\_\_\_\_

1. The LEADS Steering Committee and NCIC Advisory Policy Board requires each agency have a designated Terminal Agency Coordinator (TAC) confirmed in writing.

TAC Name: \_\_\_\_\_

Date Appointed: \_\_\_\_\_

New TAC Class Training Date: \_\_\_\_\_

In-Service Date: \_\_\_\_\_

2. Does your agency have an assistant TAC?  
(YES) (NO)

Assistant TAC Name: \_\_\_\_\_

Date Appointed: \_\_\_\_\_

New TAC Class Training Date: \_\_\_\_\_

In-Service Date: \_\_\_\_\_

3. The accuracy of LEADS and NCIC records must be double checked by a second party with verification including a comparison of the source documents, i.e. VIN, license numbers, operator's license and/or state ID information, the data in the investigative report is accurate, CCH and III information.

Is second party checking completed?  
(YES) (NO)

4. Agencies who enter records into LEADS and NCIC are responsible for their accuracy, timeliness, and completeness.

Is second party checking documented?  
(YES) (NO)

5. LEADS terminal agencies shall validate entries by their ORI as often as necessary and document the validation. Invalid entries are removed as soon as possible.

Are monthly validations completed?  
(YES) (NO)

6. Every agency, which enters records, destined for LEADS and/or NCIC must assure all records, except III records, are available 24 hours a day at the terminal, for hit confirmation purposes. This includes copies of records and/or source documents for entries made for non-terminal agencies.

Are the reports and source documents available?  
(YES) (NO)

7. Upon receipt of a hit confirmation request, the ORI of the record must, within ten (10) minutes or one (1) hour as determined by the requesting agency, furnish a substantive response, i.e., positive or negative confirmation or notice of the specific amount of time necessary to confirm or deny.

Are the hit confirmation screens used?  
(YES) (NO)

8. When confirming a hit you are to ensure:
- A. The person or property inquired upon is identical to the person or property identified in the record.
  - B. The warrant, missing person report, protection order or theft report is still active.
  - C. Obtain a decision regarding (1) the extradition of a wanted person, (2) information regarding the return of the missing person to the appropriate authority, (3) status of the protection order, or (4) information regarding the return of stolen property to the rightful owner.

Have all "hits" within the pick up radius been confirmed?  
(YES) (NO)

9. When an operational inquiry yields a hit, the terminal employee making the inquiry should note on the terminal-produced printout precisely how, when, and to whom the information was given; initial and date this notation; forward the printout to the inquiring officer or agency for retention in the case file.

Is the audit trail indicated across the printout?

(YES)            (NO)

10. Every agency, upon taking a person into custody or acquiring property after confirming the hit, must place a locate on the corresponding LEADS and NCIC record(s).

Are locates placed as required?

(YES)            (NO)

11. Prior to providing LEADS and NCIC access or service to a non-terminal agency, it must be determined the non-terminal agency is entitled to receive LEADS and NCIC access or service.

Is the non-terminal ORI verified as active before access or service is provided to them?

(YES)            (NO)

12. When running transactions for non-terminal agencies, their ORI must be used in the transaction.

Are the non-terminal ORIs being used in the transactions?

(YES)            (NO)

13. The non-terminal ORIs must be used after the message key, not at the end of the transaction.

Are the non-terminal ORIs being used appropriately in the transactions?

(YES)            (NO)

14. All agencies having terminals on the LEADS and NCIC systems are required to physically place these terminals in secure locations in the authorized agency and implement the necessary procedures to make the terminal secure from any unauthorized use.

Has the terminal(s) been placed in a secure location(s)?

(YES)            (NO)

15. All agencies intending on moving their LEADS equipment must notify LEADS at least 45 days in advance. A security inspection of the new location for the equipment must be done.

Has terminal(s) been moved without LEADS approval/inspection?

(YES)            (NO)

## **WANTED PERSON FILE COMPLIANCE**

1. Before entering a record of a wanted person in LEADS and/or NCIC, the entering agency must attempt to determine that to the maximum extent possible, extradition will be authorized for the pick up radius stated in the record.

Is extradition confirmed before a PUR is stated?  
(YES)            (NO)

2. In instances where an originating agency receives information a state will not honor the extradition of an individual, the entering agency must initiate a modify message to include in the MIS/ field of the record the words "will not extradite from..."

Are entries being modified as required?  
(YES)            (NO)

3. Certain data fields in a wanted person's record, when known, are supplemented to reflect additional information on the individual, i.e., additional social security number(s), BCI and/or FBI number(s), alias name(s), fingerprint classification, etc., or additional warrants on the same individual.

Is supplemental information added as required (packing the record)?  
(YES)            (NO)

4. A caution indicator (C) is to be added to the message key \*EWW when it is known an individual is armed and dangerous, has suicidal tendencies, has previously escaped custody, is a drug addict, or whatever is appropriate to the particular circumstances of the individual. The reason for the caution indicator must be entered first in the MIS/ field.

Is the reason for the caution indicator entered in the MIS/ field?  
(YES)            (NO)

Is the reason for the caution indicator listed first in the MIS/ field?  
(YES)            (NO)

5. Every agency, upon receiving information that an agency will not honor the extradition set forth in the pick up radius field of the warrant entry will place a locate message in the record and notify LEADS of the situation.

Are locates placed on all hits within the PUR?  
(YES)            (NO)

6. Certain offense codes (OFF) must be further defined in the MIS/ field.

Are the offense codes, when needed, further defined in the MIS field?  
(YES) (NO)

### **MISSING PERSON FILE COMPLIANCE**

1. A missing person record may be entered for the following:
  - A. A person of any age who is missing and under proven physical/mental disability or is senile, thereby subjecting himself/herself or others to personal and immediate danger (message key EMD, "D" represents disability).
  - B. A person of any age who is missing under circumstances indicating his/her physical safety is in danger (message key EME, "E" represents endangered).
  - C. A person of any age who is missing under circumstances indicating the disappearance was not voluntary, i.e., abduction or kidnapping (message key EMI, "I" represents involuntary).
  - D. A person who is missing and declared unemancipated as defined by the laws of his/her state of residence and does not meet any of the criteria set forth in A, B, C, or E (message key EMJ, "J" represents juvenile)
  - E. A person of any age who is missing after a catastrophe (message key EMV, "V" represents catastrophe victim).

Are the appropriate message keys used in these records?  
(YES) (NO)

2. A record for a person who is declared emancipated as defined by the laws of his/her state of residence can be entered in the Missing Person File provided the entering agency has documentation in their possession supporting the stated conditions under which the person is declared missing. This written documentation will aid in the protection of the individuals right to privacy. The documentation must be from a source other than the investigating police agency. Some examples are:
  - A. Written statement from a physician or authoritative source corroborating the missing person's physical and/or mental disability.

- B. Written statement from a parent, legal guardian, next of kin, or other authoritative source advising the missing person is under circumstances indicating his/her physical safety is in danger.
- C. Written statement from a parent, legal guardian, next of kin, or other authoritative source advising the missing person's disappearance is not voluntary.

Is appropriate written documentation available for each entry?  
(YES) (NO)

- 3. Every effort is made to get complete information, i.e., social security number and dental records, on EMJ entries.

In compliance?  
(YES) (NO)

### **PROTECTION ORDER FILE COMPLIANCE**

- 1. The appropriate message keys, EPO or ETO must be used.

Are the appropriate message keys used?  
(YES) (NO)

- 2. A caution indicator (C) is to be added to the message key when it is known an individual is armed and dangerous, has suicidal tendencies, has previously escaped custody, is a drug addict, or whatever is appropriate to the particular circumstances of the individual or situation. The reason for the caution indicator must be entered first in the MIS/ field.

Is the reason for the caution indicator entered in the MIS/ field?  
(YES) (NO)

Is the reason for the caution indicator listed first in the MIS/ field?  
(YES) (NO)

- 3. Certain data fields in a protection order file record, when known, are supplemented to reflect additional information on the individual, i.e., additional social security number(s), additional date(s) of birth, vehicle information, and/or additional person(s) information.

Is supplemental information added as required (packing the record)?  
(YES) (NO)

- 4. The court that issues the protection order must complete Form 10-A.

Is the court completing Form 10-A?  
(YES) (NO)

## **VEHICLE FILE COMPLIANCE**

1. A written or computer generated theft report must be on file for each entry in the vehicle file.

Is a report on file for each entry?

(YES)            (NO)

2. A loaned, rented, or leased vehicle that has not been returned cannot be entered in the file unless an official theft report is made or a field complaint results in the issuance of a warrant charging embezzlement, theft, etc.

Is a written report available for each entry?

(YES)            (NO)

3. If a felony vehicle is entered in the file, the whereabouts of the vehicle must be unknown.

In compliance?

(YES)            (NO)

4. Partial license numbers must not be entered.

In compliance?

(YES)            (NO)

5. If a license plate number exceeds eight (8) characters, enter only the last eight (8) digits in the LIC/ field. The full plate number must then be shown in the MIS/ field.

In compliance?

(YES)            (NO)

6. When only one (1) plate of a set is stolen or missing, a notation of this fact must be placed in the MIS/ field of the entry.

In compliance?

(YES)            (NO)

## **COMPUTERIZED CRIMINAL HISTORY COMPLIANCE**

1. Agencies having terminals with access to criminal history must have terminal operators screened and restrict terminal access to a minimum number of authorized employees.

In compliance?

(YES)            (NO)

2. Copies of criminal history data obtained from terminal devices must be afforded security to prevent an unauthorized access to or use of the data.

In compliance?

(YES)            (NO)

3. All terminals accessing the LEADS and/or NCIC Computerized Criminal History (CCH/III) files will maintain a manual log of all CCH inquiries (including searches) with a notation of the individual making a request for the record. All LEADS CCH and NCIC III inquiry logs will be maintained for a minimum of one (1) year.

In compliance?

(YES)            (NO)

4. Criminal justice agencies receiving a CCH response must record on the manual log any response disseminated to another criminal justice agency, or to an individual within another criminal justice agency, or to anyone legally entitled to receive such information, who is outside the original receiving agency. These logs shall be maintained for a minimum of one (1) year.

In compliance?

(YES)            (NO)

5. Radios and telephones shall not be used routinely for the transmission of CCH information beyond information necessary to effect an immediate identification or to ensure adequate safety for officers and the general public.

In compliance?

(YES)            (NO)

6. Inquiries and record requests transmitted to the CCH/III files must include the purpose code for which the information is to be used.

D. Criminal justice (purpose code "C") must be used when the CCH/III transaction is for official duties in the connection with administration of criminal justice.

E. Criminal justice employment (purpose code "J") must be used when the CCH/III transaction involves employment with criminal justice agencies only.

F. Criminal justice (purpose code "F") must be used when a CCH/III transaction involves gun permit checks.

G. Criminal justice (purpose code "D") must be used when a CCH/III transaction involves a request from a domestic court.

## TECHNICAL SECURITY ASSESSMENT

### SYSTEM DESCRIPTION

1. Is your LEADS system connected to an in-house computer system or network?  
(YES) (NO)
2. Do the PCs at your agency access the LEADS network?  
(YES) (NO)
3. Provide a diagram of your in-house network topology and LEADS connection which includes the following, if applicable:
  - A. Line types
  - B. External interfaces
  - C. Routers
  - D. Switches
  - E. Peripherals and firewalls

*This must be available the day of the audit if it applies to your agency.*
4. Explain your method for configuration changes to your network.
  - A. How are these changes documented?

### INTERNET ACCESS AND CAPABILITIES

1. Does the system incorporate Internet capabilities, dial-up access, or remote access to a network containing CJIS information?  
(YES) (NO)  
*If yes, complete the remainder of this section. If no, proceed to the next section.*
2. Is there Internet access from any other PCs on your in-house computer system or network which do not access the LEADS network?  
(YES) (NO)
3. Provide copies of all Internet connection security policies for local or interface users who maintain Internet connections or access the Internet via terminals linked to the system.
4. Provide CJIS documentation on the firewall-type devices required for users who access the Internet via terminals linked to the system.

5. Do all applied firewall-type devices meet a minimum Firewall Protection Profile as referenced in the CJIS Security Policy?  
*(Refer the following information to your network administrator or vendor. <http://csrc.nist.gov/cc/pp> and download fw\_ppa.zip for the recommended Application and Traffic Filter Firewall Protection Profiles)*
6. Provide overview documentation of advanced authentication requirements for users of Internet access/connections.
7. Provide overview documentation of all access control and integrity solutions, key exchange, etc. required for Internet access users/connections.
8. Provide overview documentation of all confidentiality policies and information security measures in place (i.e., dial-up access) for Internet access.
9. Has real-time monitoring for CJIS Network Internet access and activity been established?  
(YES) (NO)
10. Is an audit log of CJIS Network Internet access/activity maintained?  
(YES) (NO)
  - A. If yes, provide a copy of the log for the month of \_\_\_\_\_.

## TECHNICAL SECURITY

1. Provide documentation of established authentication management strategy, if any.  
*(Authentication management are the procedures established to decide who is authorized to access what system resources with what permissions, i.e., read, write, modify, delete. Technical features enforce these decisions).*
2. If transmission of criminal justice information exists over public network segments, provide a product list of encryption hardware and/or software used for records protection.  
*(A "public" network is defined as a telecommunications infrastructure that supports a variety of users. The usage of such a network by non-criminal justice entities dictates that it be considered a "non-secure" network).*
3. Provide complete documentation (specifications) of encryption methods and solutions implemented for formalized encryption management policies and procedures.  
*(Formalized key management is the documented procedures describing key generation, key distribution, key disposal, emergency procedures, key recovery and key escrow).*

## RISK ANALYSIS

Risk in the Wanted/Missing Persons, Protection Order and Vehicle files results from procedures exposing the agency to civil suit due to the lack of sufficient care in maintaining records. The risk identified is a record entered in LEADS and/or NCIC containing inaccurate and/or incomplete information; that is information which will result in an erroneous hit or will prevent a proper hit from occurring. It is also defined as the risk of invalid information remaining in the system; that is a record not being cleared when appropriate. Either risk is significant and may result in the arrest of an innocent citizen, the failure to arrest a sought after criminal, or the death of an unsuspecting officer.

### WANTED PERSON FILE

I.	Procedural Documentation for Entry	
A.	Written procedure and checklist .....	1
B.	Written procedure or checklist.....	2
C.	Well defined oral procedures .....	5
D.	No well defined procedures .....	10
II.	Type of Warrants Entered	
A.	Felony only .....	1
B.	Felony and serious misdemeanors .....	3
C.	All warrants* .....	10
	<i>*Subtract 5 points if proper validation is performed and documented.</i>	
III.	Extradition Review	
A.	Formal review of extradition by appropriate authority, (court, prosecutor, agency administrator designee), confirmed in writing.....	1
B.	Formal review, but not confirmed in writing.....	4
C.	Informal review.....	7
D.	No extradition review .....	10
IV.	Basis for Entry	
A.	Written direction, i.e., description, PUR, etc. request accompanied by original warrant .....	1
B.	Original warrant maintained by entering agency.....	2
C.	Original warrant not maintained by entering agency.....	3
D.	Oral request, by appropriate authority, confirmed in writing after entry .....	5
E.	Oral request only by appropriate authority .....	10
V.	Quality Control Procedures	

A.	CCH and/or BMV records checked and retained, entry checked by a second person, and entry message filed.....	1
B.	CCH and/or BMV records checked and retained, entry checked by a second person.....	2
C.	Entry checked by a second person and entry message filed.....	4
D.	Criminal history and/or BMV records checked and retained, entry message filed.....	5
E.	Entry checked by a second person.....	6
F.	Criminal history and/or BMV records checked and retained.....	7
G.	Entry message filed.....	9
H.	No quality control assurance measures.....	10
VI.	Validation Procedures	
A.	Agency has signed documentation to show that records are validated by contacting the appropriate court or prosecutor.....	1
B.	Agency has a written policy requiring contact with the appropriate court or prosecutor.....	3
C.	Agency has an oral policy that the court or prosecutor will be contacted as part of the validation process. Documentation does not exist to support these contacts.....	5
D.	Agency does not comply with the validation requirements.....	10
VII.	Hit Confirmation	
A.	Original warrant verified, associated records reviewed.....	1
B.	Original warrant verified.....	3
C.	Copy of warrant reviewed.....	5
D.	Card file or log book reviewed.....	7
E.	No satisfactory procedures.....	10
VIII.	Documentation of Procedures for Clearing Entries	
A.	Written procedure and checklist.....	1
B.	Written procedure or checklist.....	2
C.	Well defined oral procedures.....	5
D.	No well defined procedures.....	10
	Total score for wanted persons.....	_____

**Risk Level – Wanted Person File**

Low Risk.....less than 21 points  
Moderate Risk.....21 to 34 points  
High Risk .....more than 34 points

Within each of the individual categories, risk is assessed as follows:

Low Risk.....0 – 3 points  
Moderate Risk – procedures should be reviewed & improved where possible.....4 – 7 points  
High Risk – procedures are insufficient & must be improved immediately .....8 – 10 points

## MISSING PERSON FILE

I.	Procedural Documentation for Entry	
A.	Written procedure and checklist .....	1
B.	Written procedure or checklist.....	2
C.	Well defined oral procedures .....	5
D.	No well defined procedures .....	10
II.	Basis for Entry	
A.	Written documentation and appropriate criteria supporting stated condition of missing person .....	1
B.	Written document required for entry .....	5
C.	Oral report by officer .....	6
D.	Oral report by complainant, follow-up by officer.....	7
E.	Oral report by complainant, no follow-up by officer.....	10
III.	Entry of Juveniles	
A.	Record entered as promptly as department policy dictates to ensure maximum security effectiveness .....	0
B.	Record not entered as quickly as departmental policy dictates .....	10
IV.	Quality Control Procedures	
A.	Appropriate written documentation, additional background sources checked, NCIC entry message retained, entry second party checked .....	1
B.	Appropriate written documentation, NCIC entry message retained, entry second party checked.....	2
C.	Written documentation, NCIC entry message retained, entry second party checked .....	5
D.	Written documentation, no NCIC entry message retained, entry second party checked .....	6
E.	Written documentation, NCIC entry message retained, entry not second party checked .....	7
F.	Written documentation, no NCIC entry message retained, entry not second party checked .....	8
G.	No quality control measures .....	10
V.	Supplemental Follow-up	

A.	Review and appropriate action within 30 days (dental and other medical records) .....	0
B.	No review or appropriate action within 30 days (dental and other medical records) .....	10
VI.	Validation Procedure	
A.	Case reports reviewed, supplemental documentation reviewed and complainants contacted .....	1
B.	Case reports reviewed, supplemental documentation reviewed, and no complainant contacted .....	3
C.	Case reports reviewed, no complainant contacted.....	4
D.	Log book or card file used for validation .....	7
E.	No validations procedure .....	10
VII.	Hit Confirmation	
A.	Case report and supplemental documentation used for hit confirmation .....	1
B.	Case report used for hit confirmation .....	3
C.	Log book or card file used for hit confirmation.....	7
D.	No satisfactory procedure .....	10
VIII.	Documentation of Procedures for Clearing Entries	
A.	Written procedure and checklist .....	1
B.	Written procedure or checklist.....	2
C.	Well defined oral procedures .....	5
D.	No well defined procedures .....	10
Total score for missing persons .....		_____

**Risk Level – Missing Person File**

Low Risk.....less than 17 points  
Moderate Risk.....17 to 31 points  
High Risk .....more than 31 points

Within each of the individual categories, risk is assessed as follows:

Low Risk.....0 – 3 points  
Moderate Risk – procedures should be reviewed & improved where possible.....4 – 7 points  
High Risk – procedures are insufficient & must be improved immediately .....8 – 10 points

## PROTECTION ORDER FILE

I.	Procedural Documentation for Entry	
A.	Written procedure and checklist .....	1
B.	Written procedure or checklist.....	2
C.	Well defined oral procedures .....	5
D.	No well defined procedures .....	10
II.	Basis for Entry	
A.	Written direction, i.e., description, etc. request accompanied by original protection order and Form 10-A .....	1
B.	Original protection order and Form 10-A maintained by entering agency.....	2
C.	Original protection order and Form 10-A not maintained by entering agency .....	3
D.	Oral request, by appropriate authority, confirmed in writing after entry .....	5
E.	Oral request only by appropriate authority .....	10
III.	Quality Control Procedures	
A.	CCH and/or BMV records checked and retained, entry checked by a second person, and entry message filed.....	1
B.	CCH and/or BMV records checked and retained, entry checked by a second person.....	2
C.	Entry checked by a second person and entry message filed .....	4
D.	Criminal history and/or BMV records checked and retained, entry message filed.....	5
E.	Entry checked by a second person .....	6
F.	Criminal history and/or BMV records checked and retained .....	7
G.	Entry message filed.....	9
H.	No quality control assurance measures.....	10
IV.	Validation Procedures	
A.	Agency has signed documentation to show that records are validated by contacting the appropriate court .....	1
B.	Agency has a written policy requiring contact with the appropriate court.....	3
C.	Agency has an oral policy that the court will be contacted as part of the validation process. Documentation does not exist to support these contacts .....	5
D.	Agency does not comply with the validation requirements.....	10
V.	Hit Confirmation	

- A. Original protection order and Form 10-A verified, associated records reviewed ...1
- B. Original protection order and Form 10-A verified .....3
- C. Copy of protection order and Form 10-A reviewed .....5
- D. Card file or log book reviewed .....7
- E. No satisfactory procedures.....10

VI. Documentation of Procedures for Clearing Entries

- A. Written procedure and checklist .....1
- B. Written procedure or checklist.....2
- C. Well defined oral procedures .....5
- D. No well defined procedures .....10

Total score for protection orders.....\_\_\_\_\_

**Risk Level – Protection Order File**

- Low Risk.....less than 21 points
- Moderate Risk.....21 to 34 points
- High Risk .....more than 34 points

Within each of the individual categories, risk is assessed as follows:

- Low Risk.....0 – 3 points
- Moderate Risk – procedures should be reviewed & improved where possible.....4 – 7 points
- High Risk – procedures are insufficient & must be improved immediately .....8 – 10 points

**VEHICLE FILE**

- I. Procedural Documentation for Entry
  - A. Written procedure and checklist .....1
  - B. Written procedure or checklist.....2
  - C. Well defined oral procedures .....5
  - D. No well defined procedures .....10
  
- II. Basis for Entry
  - A. Officer’s report (written or oral), complainants written acknowledgment, and/or warrant required .....1
  - B. Officer’s report (written or oral) .....3
  - C. Oral report by complainant, officer follow-up within 12 hours .....6
  - D. Oral report by complainant, no follow-up .....10
  
- III. Quality Control Procedures
  - A. Owner verification (title viewed and BMV checked), entry vs. report checked by a second person, entry message filed .....1
  - B. BMV checked, entry vs. report checked by a second person, entry message filed .....3
  - C. Entry vs. report checked by a second person, entry message filed .....4
  - D. BMV checked, entry message filed .....5
  - E. Entry vs. report checked by a second person .....6
  - F. BMV checked .....7
  - G. Entry message filed .....9
  - H. No quality assurance measures .....10
  
- IV. Validation Procedures
  - A. Agency has documentation with source document that records are validated by contacting the victim/complainant and/or owner .....1
  - B. Agency has written policy requiring contact with the victim/complainant and/or owner .....3
  - C. Agency has an oral policy that the victim/complainant and/or owner will be contacted as part of the validation process. Documentation does not exist to support these contacts .....5
  - D. Agency does not comply with validation requirements .....10
  
- V. Hit Confirmation

- A. Theft report and other supplemental information used for hit confirmation .....1
- B. Theft report only .....4
- C. Log book or card file used for hit confirmation.....8
- D. No satisfactory procedure .....10

VI. Documentation of Procedures for Clearing Entries

- A. Written procedure and checklist .....1
- B. Written procedure or checklist.....2
- C. Well defined oral procedures .....5
- D. No well defined procedures .....10

Total score for vehicles.....

**Risk Level – Vehicle File**

- Low Risk.....less than 13 points
- Moderate Risk.....13 to 28 points
- High Risk .....more than 28 points

Within each of the individual categories, risk is assessed as follows:

- Low Risk.....0 – 3 points
- Moderate Risk – procedures should be reviewed & improved where possible.....4 – 7 points
- High Risk – procedures are insufficient & must be improved immediately .....8 – 10 points

**3.4 LEADS OPERATOR CERTIFICATION SYSTEM**

The LEADS Operator Certification System gives LEADS terminal agency coordinators (TAC) the ability to re-certify their operators on-line via the workstation.

The first Sunday of each month your agency will receive a teletype listing the LEADS operators needing recertification during the current month. When an operator passes the test their records will automatically be updated as having been re-certified. If the operator does not test during the month their re-certification is due, the operator will be made in-active. The TAC must contact LEADS Control to have the operator re-activated after completing the re-certification test. If it is the first time an operator is taking the test, the TAC must contact LEADS prior to retrieving the test. The operator's name, social security number and operator's license or identification number must be added to the tracking system before a test may be retrieved.

The examination, which is requested through the LEADS workstation, randomly selects 50 questions from a bank of 400 questions. The test is taken by submitting the answers via an answer screen. After the answers are transmitted, the final grade, correct answers and missed questions will immediately be returned.

Operators have 72 hours to take the test once retrieved. Failure to take the test within 72 hours will result in a failing grade. Operators will be permitted a total of three (3) opportunities to pass the test. If the operator has failed to pass the test, it is the TAC's responsibility to provide remedial training. The test can be re-taken after 48 hours. After three (3) failures, the operator will not be permitted to use LEADS.

After three (3) months, the agency administrator can submit documentation of steps taken to train and qualify that employee. The employee will be given a fourth, and final, opportunity to certify/re-certify.

### **3.4.1 Exam Retrieval**

*Full certification* is required to process any type of file inquiry or update available to the agency via the LEADS. All TACs are to be fully certified. To retrieve and print a *full certification* 50 question exam key LTR. and the operator license number of the person to be tested. Example:

LTR.OLN#(TRANSMIT)

A *conditional exam* will provide a set of 50 questions taken from Section 1 through 7 of the LEADS manual, part 1 of the NCIC manual, and the LEADS Administrative Rules. Conditional certification is designed for agency personnel who have occasion to sit desk relief for a LEADS operator or whose duties (i.e. record clerk, jailer, detective, etc.) require them to process inquiries through the LEADS in order to properly administer those duties. To retrieve and print a conditional exam key LTR., the operator license number of the person to be tested followed by a period, then the letter "C."

*Example:*

LTR.OLN#.C (TRANSMIT)

An exam for Mobile Data Terminal (MDT) users is also available. To retrieve and print this test, key LTR., the operator license number of the person to be tested followed by a period, then the letter "M."

*Example:*

LTR.OLN#.M(TRANSMIT)

An exam for Department of Rehabilitation and Corrections (DRC) users is also available. To retrieve and print this test, key LTR., the operator license number of the person to be tested followed by a period, then the letter "D."

*Example:*

LTR.OLN#.D(TRANSMIT)

### 3.4.2 Grading the Exam

To retrieve the blank screen used to enter exam answers, key the following:

LTS.(TRANSMIT)

A sample of this screen is shown below. Enter the operator license number (SSN) of the person being tested. Next, type the operator's last name, then full first name and middle initial. Make sure none of the periods in the operator name field are deleted after keying the name. Enter the answers in the spaces provided. Lastly, enter the social security number of the TAC/examiner giving the test. Move the cursor below the last line and transmit.

LEADS CERTIFICATION EXAM FOR OPERATORS

LTG.

06/01/94

OPERATOR OLN/.....

OPERATOR LAST NAM/..... FIRST NAM/..... DOB/yyyy/mm/dd

001-. 002-. 003-. 004-. 005-. 006-. 007-. 008-. 009-. 010-.  
011-. 012-. 013-. 014-. 015-. 016-. 017-. 018-. 019-. 020-.  
021-. 022-. 023-. 024-. 025-. 026-. 027-. 028-. 029-. 030-.  
031-. 032-. 033-. 034-. 035-. 036-. 037-. 038-. 039-. 040-.  
041-. 042-. 043-. 044-. 045-. 046-. 047-. 048-. 049-. 050-.

TERMINAL AGENCY COORDINATOR (TAC) SOC/.....

**Note:** Once the exam has been graded, for a new operator taking the test for the first time, a computer generated message will be returned to you. This form must be completed with the information requested and sent back to LEADS Control.

### 3.4.3 LEADS OPERATOR TRACKING SYSTEM

The LEADS Operator Tracking System is designed to protect LEADS from unauthorized use and keep track of transactions for each operator. Each operator must login before using the workstation and logout whenever the workstation is unattended.

A user-ID identifies each LEADS operator. Your user-ID will be the same as your operator license number (OLN) or state identification number. If the operator does not have an OLN or state ID, LEADS Control will assign a user-ID to the operator. If you access LEADS from more than one agency, you will need a unique user-ID for each agency. User-IDs for additional agencies are created by adding one letter to the end of your OLN. For example: ZZ123456 would be used at the first location. If you are employed at a second agency, your user-ID would be ZZ123456A. A password prevents other people from using your user-ID.

New operators must use the default password, "NEW" when they initially login following certification. Passwords must be at least five (5) characters and no more than eight (8) characters in length. Passwords can contain numbers and uppercase letters. Passwords cannot be reused. The system allows you to change your password after 10 days and requires it be changed after 35 days. Examples of valid passwords are: NASDAQ3, COMEX, NOT2BAD.

When a login is required, the system will display the message: Enter UserID/Password. If the cursor is not to the immediate right of the start of entry (SOE), press transmit. Starting at the SOE, enter your user-ID, a slash (/), your password, then transmit. If you make a mistake, the message: Enter User ID Password will be re-displayed.

If your password has expired, you are required to *change* your password. The system will display the message:

Password Expired; Enter New Password

Enter only a password of your choice in accordance with the requirements above and transmit. (You do not need to use your operator license number when creating a new password.)

Once you have entered a valid password, you will be prompted to enter only your password a second time to confirm the change. The system will display the message:

```
Re-Enter New Password
```

Enter your password only, exactly as before and transmit. After you successfully login, a short message will appear which contains your session number, name, date and the time. The attended mode will have been cleared.

*Login* - Below is an example of how someone with a user-ID of ZZ123456 would login for the first time and then create the password SAMPLE.

1. Key the user-ID and password at the SOE and transmit.

```
>ALL DATA ACCESSED THROUGH THE NCIC/LEADS IS PROTECTED  
>BY FEDERAL/STATE LAW AND IS TO BE USED EXCLUSIVELY BY  
>CRIMINAL JUSTICE AGENCIES FOR CRIMINAL JUSTICE PURPOSES
```

```
>Enter UserID/Password  
>ZZ123456/NEW
```

2. Key in the password SAMPLE at the SOE and transmit.

```
>Password Expired; Enter New Password  
>SAMPLE
```

3. Key in the Password again, exactly as before, and transmit

```
>Re-enter New Password  
>SAMPLE
```

4. When the workstation is logged on, a message with the following format is printed:

```
LEADS Session #001  
Operator: LAST,FIRST MI  
Date:      2000/10/25  
Time:      08:00:00
```

```
MESSAGES DELIVERED ATTENDED MODE CLEARED
```

*Logout* - Whenever a workstation is unattended, it is to be logged out to prevent unauthorized use. To logout of LEADS, enter message key LOGOUT. and transmit. A message containing your user-ID, date and time will be displayed and the attended mode will be cleared.

1. When the workstation is logged out, a message with the following format is displayed:

```
>LEADS Input Session Closed
>2000/10/25 18:00:00
>Enter UserID/Password
>
MESSAGES DELIVERED ATTENDED MODE CLEARED
```

### **3.4.4 CCH/LEADS CERTIFIED OPERATOR RECORDS**

Periodically, your agency will receive a computer generated message indicating it is time to audit your department's personnel for CCH and LEADS training or certification. After pulling up a listing of your agency personnel, please follow the instructions at the top of each list.

To retrieve a list of your agency personnel who are CCH certified, the TAC must log-on to LEADS and BCI&I then enter:

```
CHAUD. ( TRANSMIT )
```

To retrieve a list of your agency personnel who are LEADS certified, the TAC must log-on to LEADS and BCI&I then enter:

```
DPAUD. ( TRANSMIT )
```

If you have any questions regarding this procedure, contact BCI at 740-845-2364 or /OHBCI0000.

A copy of the LEADS Operator Update form can be found in the back of this section.

### **3.4.5 COMPUTERIZED CRIMINAL HISTORY (CCH) TESTING**

Refer to the BCI & I Training Manual for Computerized Criminal History/Civilian Applicant Card Processing for the CCH testing procedures.

**LEADS OPERATOR UPDATE FORM**

*Please use this form each time there is a change in your operator list.*

MAIL TO: OHIO LEADS  
 PO BOX 182075  
 COLUMBUS OH 43218-2075

DATE: \_\_\_\_\_

TAC: \_\_\_\_\_

ORI: \_\_\_\_\_

AGENCY: \_\_\_\_\_

ACTION TYPE:  Add/Delete/ Modify	NAME: Last, First, MI	DATE OF BIRTH	OLN # / STATE ID # / LEADS ASSIGNED #	ORI*	TYPE OF CERTIFICATION (TAC, FQO, INQ, MDT)	DATE CERTIFIED

\*The ORI listed must be the ORI associated with the operator’s certification. This may be a different ORI than the agency submitting the form, since MDT service may be provided by a different agency.

### 3.5 JOB DESCRIPTION - LEADS TERMINAL AGENCY COORDINATOR (TAC)

#### **4501:2-10-04 LEADS Terminal Agency Coordinator (TAC).**

(A) A LEADS terminal agency coordinator, hereafter referred to as TAC, shall be appointed by each terminal agency administrator. The TAC must be fully certified as a LEADS operator and have supervisory authority over the operation of LEADS approved equipment. The TAC is directly responsible to the agency administrator for the operation of LEADS.

(1) Duties: LEADS terminal agency coordinator

- (a) Responsible for the training of LEADS terminal operators in all facets of terminal operation and other affected personnel as to the operational capabilities of the LEADS. Ensure each operator reviews training materials and is recertified every two years.
  - (I) shall attend the new TAC indoctrination training
  - (II) shall attend the minimum two in-service training sessions and others as scheduled.
  - (III) shall initially (within six months), train, functionally test and affirm the proficiency of terminal (equipment) operators.
  - (IV) Shall participate/attend any audit of the employing agency.
- (b) Responsible for the proper completion of the monthly records validations.
- (c) Maintain all documentation from LEADS, including but not limited to:
  - (I) newsletters;
  - (II) LEADS computer messages;
  - (III) manuals; and
  - (IV) lesson plans
- (d) Maintain agency level records of LEADS certified operators and notify LEADS of any changes on the prescribed form provided by LEADS control.
- (e) Review all entries within a reasonable time frame for accuracy; modify/remove entries as needed.
- (f) Know the location and use of all LEADS equipment within the agency.
- (g) Biennially provide the functional retesting and reaffirm the proficiency of terminal operators in order to assure compliance with LEADS/NCIC policy and regulations.

- (2) Requirements:
- (a) Knowledge of the responsibilities, functions, organization structure, purpose and aims of the agency.
  - (b) Knowledge of methods, procedures and programs in law enforcement.
  - (c) Knowledge of security and computer personnel working directly or indirectly with the computer system.
  - (d) Knowledgeable of the NCIC, NLETS and LEADS rules, regulations, and guidelines. This knowledge includes, but is not limited to, being familiar with what services are available, user agreements, and non-terminal agency agreements.
  - (e) Knowledge of all procedures concerning broadcast messages and their proper use.
  - (f) Knowledge and administration of the general maintenance of the equipment.

### **3.5.1 ADDITIONAL TAC RESPONSIBILITIES**

The TAC will also serve as the Point of Contact (POC) for any security violations or concerns within the department. These responsibilities include:

- Serve as the security point of contact for the Information Security Officer (ISO) at the local agency.
- Know who is using the equipment and how the equipment is connected to CJIS systems.
- Ensure that no untrained personnel are using CJIS system terminals.
- Ensure that hardware has the appropriate security measures in place.
- Keep the ISO informed of security incidents.
- Support policy compliance at the local agency in partnership with the ISO.

### **3.6 AGENCY ADMINISTRATOR INFORMATION - NON-TERMINAL AGENCIES**

LEADS is now responsible for the signing of the agreements with the non-terminal agencies. LEADS shall provide the non-terminal agency with a copy of the participation agreement, a copy of the LEADS Administrative Rules, a copy of Section 1.8 of the LEADS Operating Manual

covering Validation, and training materials applicable to LEADS Practitioners (road officers, secretaries, clerks, etc.)

Terminal agencies may disseminate information to a non-terminal agency providing the non-terminal agency is in good standing with LEADS. The non-terminal agency ORIs must be used in transactions run for those agencies (see Section 3.2.1). When using these ORIs the transaction will be accepted or rejected, if the transaction is rejected, the agency is not in good standing with LEADS and LEADS information should not be disseminated to the non-terminal agency in question. If the ORI is rejected the following message is generated:

REJ NOT AUTH

### **3.7 MESSAGE GUIDELINES**

All traffic over the system must be in the prescribed message form. Unnecessary messages with superfluous verbiage or embellishments are prohibited.

Information of no value to the receiving agency must be avoided, i.e., the address or telephone number of parents reporting a runaway child are of no value to another department. The originating department, not the parents, will be notified of any apprehension.

Avoid expressions such as "Arrest and Hold", "Hold for Investigation", "Hold and Notify", "Detain for this Department", "Wanted as Suspect", etc. The name of the crime is to be clearly specified and if a warrant has been issued, it is to be entered in the LEADS/NCIC system.

In view of the many persons who can receive messages, the use of non-standard abbreviations must be avoided. Keep in mind many abbreviations which may be common within one department or in one state can be entirely unknown and confusing to another department or state. Departmental radio codes must not be used.

It is imperative departments originating any type of "want message", cancel the message when it no longer applies. Messages can be canceled only by the originating department. *Do not resend the original message when canceling.*

Departments apprehending a wanted subject or recovering stolen or wanted property must send a notification to the originating agency, reporting the apprehension or recovery using the prescribed hit confirmation screen. The originating department must then cancel their outstanding messages and clear their LEADS/NCIC file entry.

Ohio agencies may receive an incoming administrative message coming from a state that uses a "Control Field". A control field is a ten-digit alpha-numeric identifier used by some states instead of "for the attention of", or for routing purposes to a specific person or section. The control field will be on the sixth line of the message and is preceded by an asterisk (\*) and consists of ten digits.

Ohio does not use a control field, except in response to an incoming message. With a control field, you must use the identical field on your reply message. It goes to the right of the header. An asterisk (\*) separates the control field from the header.

### 3.7.1 MESSAGE CONSTRUCTION

Each message sent over the LEADS consists of six basic lines of information. Based on the information being sent and the message type, some slight variations may exist from one message to another. However, each message will have at least five of the following six elements present in order to be valid. A simple way to remember all six message elements is to ask yourself the question -- Do I have all the P.A.R.T.S.?

Message Header - Line 1

Message Preamble - Line 2

Message Address - Line 3

Message Reference - Line 4

Message Text - Line 5

Message Signature - Line 6

A step by step explanation of how a message is to be constructed can best be described by using the following original message type example:

- (1) /OHALLPSCO
- (2) MSG 1459
- (3) ALL DEPTS CENTRAL OHIO
- (4) ARMED ROBBERY
- (5) 0800 EDT 063094 DRUG STORE EAST MAIN STREET THIS CITY. ONE  
SUBJECT ARMED WITH REVOLVER. LAST SEEN HEADING WEST ON  
RT.40 DRIVING LATE MODEL GENERAL MOTORS PRODUCT
- (6) PD REYNOLDSBURG OH 0835 EDT JOE

### **3.7.2 Message Header - Line 1**

The message header (ORI) is a nine-character NCIC assigned agency identifier which directs the message to its proper location(s). A message can be addressed to a total of five individual agencies by using the ORI for each agency. ORI's are to be entered on line 1. The first ORI must be preceded by a slash (/). The remaining are separated by commas. There is no punctuation after the last entry. *Example:*

/OHOHP0000,OH0250100,OH0251100,OH0250000,OH COP0000

If you wish to obtain a copy of the message for your files, key in your ORI as one of the individual headers you are using to send the message.

When using Ohio broadcast code messages, i.e., OHALLTERM or QUAD, more than one Ohio header may be used. You may also use the Ohio broadcast codes in conjunction with an individual agency ORI. If you want to direct the message to another state at the same time simply place the two letter state code identifier after the ALLTERM/QUAD header. Do not use a nine digit ORI for QUAD and ALLTERM requests to other states, use only the two character header.

*Example:* /OHALLTERM, PA

Note: The sending of ALLTERM and QUAD messages to other states is prohibited.

### **3.7.3 Message Preamble - Line 2**

This line consists of the originating agency's message number and is for original messages only.

When the message is delivered, the computer will add a line indicating the sending agency's ORI, automatic message number, the time and date.

### **3.7.4 Message Address - Line 3**

This is the name of the department(s) or agency(s) who is to receive the message. If it is desirable to send the message to a specific section or person within a department, it can be added on the same line, i.e., SO COLUMBUS OH DEP. SMITH TRAFFIC BUREAU. (Note: If you are responding to an out-of-state message containing a control field header, refer to Section 8.3.2 of this manual for additional information.)

### **3.7.5 Message Reference - Line 4**

Describe the reason the message is being sent, i.e. escape, armed robbery, etc., see example in Section 3.7.

### **3.7.6 Message Text - Line 5**

This is to be a brief description of the action being requested and/or details of information being supplied. If the message refers to a crime, the following data is requested in this line:

*Type of Crime;*

*Time and location of crime.* Use military time - 0100 = 1:00 A.M. and the zone - EST = Eastern Standard Time or EDT = Eastern Daylight Time.

*The name and/or description of the person(s) wanted.* Include the following: race, sex, age, height, weight, hair, eyes, complexion, build, scars, marks, tattoos and clothing description.

A minimum description of the motor vehicle is to include: color, year, make, body style, and license number. Two tone colors are listed with the upper most color first. Include other distinguishing features, i.e., right front fender missing, headlight out, driver's door dented, etc.

Warrant information is to include the specific crime of the wanted individual, and whether or not the person is charged with a felony or misdemeanor. This section must contain a statement on extradition for all out of state messages.

### **3.7.7 Message Signature - Line 6**

This line consists of three entries. The first entry is the complete agency name to include department, city and state. The second entry is the time the message is sent, and the time zone. The third entry is the initials of the operator. If a message is relayed by another department, precede the entries described above with the abbreviation for "Relayed" (RLYD).

*Example:* RLYD OHIO STATE HIGHWAY PATROL MEDINA 0900 EDT RLG

## **3.8 MESSAGE TYPES**

Listed in this section are examples of the different types of messages that can be sent over the LEADS. Associated with each message type example is a brief definition.

### **3.8.1 Added Message**

An added message is sent to supplement a previous message. The type of message is entered in the second position of line 2. Also, line 4, message reference, must be included.

- (1) /OHALLPSCO
- (2) MSG 1459 ADDED
- (3) ALL DEPTS CENTRAL OHIO
- (4) REF 1459 OH0250800 063094
- (5) SUBJECT W/M 25 510 180 BLK AND BLU  
WEARING FLIP BRIM CAP, YELLOW POLO SHIRT, KHAKI TROUSERS.  
ARMED WITH SHORT BARREL, BLUE STEEL SMALL CALIBER REVOLVER.
- (6) PD REYNOLDSBURG OH 0915 EST JOE

### **3.8.2 Part Cancel**

A part cancel is sent to cancel part of the original message. The type of message is entered in the second position of line 2.

- (1) /OHALLPSCO
- (2) MSG 1459 PART CANCEL
- (3) ALL DEPTS CENTRAL OHIO
- (4) REF 1459 OH0250800 091687
- (5) SUBJECT ABANDONED STOLEN TWO TONE BLUE 70 PONT 2D LIC  
ABC123, VIN/262370X105007
- (6) PD REYNOLDSBURG OH 1000 EST JOE

### **3.8.3 Cancel**

A cancel is a message which cancels a previous message. The type of message is entered in the second position of line 2.

- (1) /OHALLPSCO
- (2) MSG 1459 CANCEL
- (3) ALL DEPTS CENTRAL OHIO
- (4) CANCEL 1459 OH0250800 063094
- (5) ONE SUBJECT APPREHENDED
- (6) PD REYNOLDSBURG OH 1310 EST PAM

### **3.8.4 Reply**

A reply is a message in response to an original message received by your department. The type of message is entered in the second position of line 2.

- (1) /OH0250800
- (2) MSG 1459 REPLY
- (3) PD REYNOLDSBURG OH
- (4) REF 1459 OH0250800 063094
- (5) OWNER NOTIFIED. WILL CONTACT YOUR DEPT RE DISP.
- (6) PD COLUMBUS OH DET JONES AUTO SQUAD 1120 EST KLF

### **3.8.5 Correction**

A correction is a message sent to correct information in the original message. The type of message is entered in the second position of line 2.

- (1) /OH0250400,OHBCI0000
- (2) MSG 1459 CORRECTION
- (3) PD GAHANNA OH, BCI BUREAU OF CRIMINAL INVESTIGATION
- (4) REF 1461 OH0250800 063094
- (5) CORRECT DOB 112348
- (6) PD REYNOLDSBURG OH 1301 EST JAN

### **3.8.6 Follow-up**

A follow-up is a message requesting an answer to an original message. The type of message is entered in the second position of line 2.

- (1) /OH0250400,OHBCI0000
- (2) MSG 1462 FOLLOW UP
- (3) PD GAHANNA OH, BCI BUREAU OF CRIMINAL INVESTIGATION
- (4) REF 1461 OH0250800 063094
- (5) ADVISE WHEN YOU HAVE SUBJECTS
- (6) PD REYNOLDSBURG OH 1450 EST JAN

### **3.8.7 Resend**

A resend is a message requiring the original message be sent again in its entirety. Normally the reason for receiving one of the last two types of messages means the original message was never received by the central processor.

### 3.8.8 Miscellaneous Messages

There are two messages in this group, Attempt-To-Locate (ATL) and Attempt-To-Contact (ATC). These messages are to be used only when all other means have failed and limited to cases of extreme emergency i.e. foul play is suspected or known; death or serious illness messages; or delivery of military orders. An ATL message is to give the area of travel, including vehicle description, time of departure, routes of travel and any known stopovers. This information will be entered in the text (line 5) of the message.

### 3.8.9 Transmitting Multi-Page Messages

1. Move your cursor to the home position on the screen. Clear the screen of all information.
2. Type PAGE.1 on the screen, return carriage (ENTER key).
3. Type in a slash followed by the agency destination ORI. A maximum of five ORI's may be entered on this line. If you wish to receive a copy of the message sent, you must include your nine character agency identifier as one of the five ORI's on this line. Return the carriage (ENTER key).
4. Type in the text of message.
5. At the end of the first page, place an asterisk (\*) and transmit. Your workstation will respond with: PAGE.2 at the top left of the monitor. Continue message text where you stopped on PAGE.1. DO NOT RE-ADDRESS WITH THE AGENCY ORI(S).
6. Continue steps 4 and 5, if necessary, through six (6) pages. This is the maximum number of pages permitted. No matter how many pages are sent, your message cannot contain more than 2,200 characters.

*Example:*

```
PAGE.1(Enter)  
/OHLEADSCY,OHOHP0098(Enter)  
TEXT OF MESSAGE*(TRANSMIT)
```

The workstation will respond with:

```
PAGE.2  
(continue typing your message where you left off)
```

7. To end the multi-page message, press the F12 key or icon without using the asterisk (\*), and your workstation will send the total message all at one time. The workstation will

respond with "MESSAGE ROUTED TO:" followed by the agency ORI(s) to which you addressed your message.

*Example:*

```
MESSAGE ROUTED TO:  OHLEADSCY,OHHP0098
OHLEADSCY,OHHP0098 059 10:31:22 12/13/95
TEXT OF MESSAGE
ANYTOWN POLICE DEPARTMENT
```

If you wish to retrieve Page 1 of a multi-page message for correction or change, type in: PAGE.R1, do a carriage return and transmit. The message in PAGE.R1 will appear on the monitor. Place the Start-Of-Entry symbol in front of the "PAGE" number. Make the necessary corrections or changes, including deletion of R in PAGE.R1, move the cursor to the end of the page, type an asterisk (\*) and transmit.

Do the same for pages 2, 3, 4, etc. If you are in the middle of a multi-page message, and wish to do a retrieval of a page, note the page number of the last page you were working on before the retrieval. This number must be entered at the top left of the screen before you continue with the multi-page message.

Note: If you wish a copy of the message for your records be sure to enter your ORI in the header.

### **3.9 BROADCAST MESSAGE CODES**

To simplify the sending of a message to more than one agency or department, Ohio law enforcement and criminal justice agencies are grouped into areas, or quadrants. More than one broadcast message code may be used in a header. (Individual agency ORIs may be used with the broadcast codes, providing the individual agency ORI is listed **first**, followed by the broadcast message code). Each agency resides in a specific quadrant (see section 3.9.1). Messages will be sent to all criminal justice workstations in the areas as defined by the quadrant broadcast codes listed.

OHALLPSNW - northwest quadrant of Ohio

OHALLPSNE - northeast quadrant of Ohio

OHALLPSSW - southwest quadrant of Ohio

OHALLPSSE - southeast quadrant of Ohio

OHALLPSCO - nine county central Ohio area (These workstations also remain in the respective assigned quadrant.)

- OHALLOHPD - all Highway Patrol District Headquarters and the Training Academy (The sending agency will be notified if any workstation is inoperative.)
- OHALLOHPT - all Highway Patrol workstations individually, (The sending agency will be notified if any workstation is inoperative.)
- OHALLOHPS - all Highway Patrol workstations at posts with scales.
- OHALLGHQT - all Highway Patrol workstations at the Highway Patrol General Headquarters.
- OHALLOHP# - (replace the # with a Highway Patrol District number) all Highway Patrol workstations within the designated district.
- OHALLTERM - all Police, Sheriff, Highway Patrol and other criminal justice workstations (Use this code only for urgent and important messages when it is necessary for every criminal justice agency in the state be alerted.)
- OHALLLAKE - along the Lake Erie shore
- OHALLRIVR - along the Ohio River shore
- OHALLIS70 - along Interstate 70
- OHALLIS71 - along Interstate 71
- OHALLIS75 - along Interstate 75
- OHALLIS77 - along Interstate 77
- OHALLSHRF - all Sheriff's agencies individually who have LEADS access
- OHALLPLCE - all Police agencies individually who have LEADS access
- OHALLTNPK - all agencies along the Ohio Turnpike. This code is only used by the State Highway Patrol Berea District Headquarters (Turnpike) to notify agencies of road conditions, etc.
- OHALLCNXX - all LEADS users in county XX  
(XX = county number 01 through 88)
- OHADJCNXX - all LEADS users in county XX and all adjacent counties  
(XX = county number 01 through 88)

### **3.9.1 LEADS Quadrant Broadcast Boundaries**

The LEADS broadcast boundaries map is included (see figure 3.9.1) to provide a visual of the exact geographic area of the state to which the various quadrant broadcast covers. Also identified are the counties in each quadrant.

This will assist the user to determine if the use of the quadrant broadcast is actually necessary. Many times the purpose can be accomplished by addressing multiple workstations as opposed to the broadcast identifier.

### **3.10 MESSAGE RETRIEVAL**

If a message cannot be received at a workstation, the message will be held by the LEADS central processor. When the receiving workstation is ready to receive messages, it can request the messages from the central processor. This situation may occur when the LEADS operator at the receiving workstation is busy or using the workstation to prepare a message. (attended mode)

A limited number of messages received at the workstation can be retrieved by the operator. The number of messages retrievable is dependent upon several factors. The primary factor is the volume of traffic sent by the transmitting workstation. All messages in a series, i.e. numbers 1 through 10, may not be retrievable at a given time because of the volume of traffic sent by the transmitting workstation.

### **3.10.1 How to Retrieve a Message**

Each LEADS message handled by the central processor and received by a workstation will contain a message sequence number. This number can be used at a later time to retrieve an additional copy of the message. The message consists of the message key RT followed by a period and the message number to be retrieved. The format for retrieving a single message follows:

To determine the last message number received by your workstation, make the following inquiry.

```
RT.N(TRANSMIT)
```

The message response will be the last message number sent by the central processor. Use the number in the following format to retrieve the last message received.

```
RT.(message number)(TRANSMIT)
```

### **3.10.2 Message Queues**

If the system has a message to send to a workstation, and the workstation is busy or inoperative, the message will be held until the workstation is available. To release all messages being held, click on the "MSG" icon or CTRL w. It is the responsibility of each LEADS operator to check all messages and message numbers received to verify the information is complete. If a workstation is busy and the message is not retrieved within three minutes of the audible signal, the three minute timer expires and the first queued message is automatically released. Additional queued messages must be released by clicking on the "MSG" icon or CTRL w. *It is advisable to perform a transaction every 15 minutes to insure your workstation is operational.*

### **3.10.3 How to Reroute a Message**

Each administrative message handled by the central processor and received by a workstation will contain a message sequence number. This number can be used to reroute a copy of the message to another workstation. The format for rerouting an administrative message is as follows:

```
RT. 3.OH0250000 (TRANSMIT)
```

Message number 3 will be routed to workstation OH0250000.

### **3.11 ERROR MESSAGES**

When data is entered incorrectly or a transmission failure occurs, the LEADS central processor will generate an error message to the sending workstation. Listed below are the various error messages received as a result of a message switching error. Associated with each error message are the corresponding steps to be taken to correct the error.

*Destination Code Error* - The processor will respond with this error message when there is an error in the header of the message being sent. For example: If you are sending a message to three agencies, and the first ORI in the header is incorrect; the other two ORIs will receive the message, and you will be notified by the system the message has been routed to them. You will also be notified you have used an improper header in your address, and it will list the incorrect ORI. You will then need to address the message to the correct ORI and resend it.

*REJ Header Error* - This message is sent by the processor if more than 51 characters appear in the message header line. The message will not be processed by the central computer. Correct the header by reducing the number of characters, and resend the message.

Message headers can be addressed to up to five individual workstations. If more than one header is used, there must be a comma placed between each header. In a broadcast message, only one header is permitted, see Section 3.7.1.

*REJ Message Too Long* - This message is sent by the central processor if a multi-page message exceeds 4000 characters. The message will not be processed and is to be shortened and resent.

### **3.12 RESTRICTIONS**

The system must not be used for the following types of messages:

1. Social announcements, i.e., holiday messages, retirements, convention notices. Seminars or training classes are not permitted over NLETS.
2. Recruiting of personnel.
3. Messages in which the complainant is interested only in the recovery of property.

4. Attempts To Locate vehicle (Breach of Trust) without warrant. For the protection of the arresting officer, messages are not to be dispatched until a warrant is secured.
5. Excessively long messages.
6. Transmission of subpoenas.
7. Use of vehicle registration or drivers license information obtained via LEADS is limited to law enforcement, criminal justice or BMV purposes only. Curiosity inquiries are forbidden.
8. Messages supportive or in opposition to political issues or announcement of meetings relative to such issues.
9. Messages supportive or in opposition to labor/management issues or announcements relative to such issues.
10. Messages supportive or in opposition of legislative bills.
11. Messages relating to requests for information concerning salary, uniforms, personnel, or related items which can be routinely obtained by correspondence or means other than LEADS/NLETS.
12. Messages relating to the advertisement or sale of equipment.
13. Individual listing of items stolen is prohibited. A general description of property is permitted.
14. Radio codes in messages must not used.
15. Excessive wordage and exotic characters, (i.e., \*\*\*), must not be used.

### **3.12.1 All Points Bulletins - APB (nationwide)**

The following restrictions control the sending of APB's. When sending an APB, users are urged to carefully consider if there is a necessity to send the message to all states. If the message pertains to a geographical area of the United States, i.e., east coast Sunbelt, the user is to seriously consider the use of a regional broadcast which can more narrowly focus on the states who could provide assistance. See Section 8.14.1 of this manual for a listing of NLETS broadcast areas and restrictions of use.

### **3.12.2 Ohio ALLTERM, QUAD and Other Messages**

The sending of ALLTERM, QUAD and other messages to Ohio LEADS agencies must be restricted to criminal justice business only.

ALLTERM messages must not be transmitted on the LEADS when the subject matter would be of interest only to agencies in the close geographical area. Use all county, contiguous counties or quadrant broadcasts in these circumstances.

### **3.13 FORMATTED SCREENS**

LEADS has implemented the formatted screen programs for the purpose of entering, locating, adding, clearing, and canceling items and persons in the LEADS/NCIC files.

These files include: license plates, vehicles, vehicle parts, boats, guns, articles, securities, missing persons, unidentified persons, wanted persons, detainer, protection orders, and immobilized/towed vehicles.

The modify function is not included in these formats. To modify an entry, use past procedures outlined in the LEADS and NCIC Manuals.

To use the formatted screens, place an asterisk (\*) on the screen followed by the desired message key and transmit. Example of format used to call up a wanted persons screen:

\*EWW (TRANSMIT)

*Note:* A pound sign (#) will replace the asterisk (\*) once your message key is transmitted. See examples of this in each section with formatted screens.

Definitions of the various formatted screen message keys appear in the Auto Alert (Section 4), Wanted, Missing and Unidentified Persons (Section 6), and Communications with NCIC (Section 7).

After the message key has been entered, the entire format will immediately appear on the screen. The operator must then complete the fields in the format using the proper codes. A listing of the codes used in each data field is defined in the appropriate sections of the NCIC Code Manual.

*Note:* Before you transmit your screen, you must place your cursor beyond the period on the last line of the screen format.

No punctuation is permitted in screen formats, with the exception of a dash in the OCA field, a comma in the name field of a wanted or missing person entry, and hyphen used to separate the serial numbers in all formats used in consecutive numbered articles and securities.

The screen formats contain five different symbols in the various fields. Each symbol has a specific meaning:

A series of underscores ( \_ ) means this is a required field.

A series of commas (,) means at least one of the fields is required.

A series of asterisks (\*), plus signs (+), or equal signs (=) means if one field is used, all fields containing this symbol are required.

The captions containing asterisks, plus signs, and equal sign symbols categorize groups of data. A field containing no symbol is an optional field.

If the fields are entered correctly, LEADS will process the entry and place it in file. Entries which qualify for NCIC will automatically be sent to NCIC. NCIC will respond with the NCIC Identification Number (NIC).

On wanted and missing persons entries, if all fields are entered correctly, LEADS will process the entry and return an assigned LEADS Identification Number (LID) in addition to the NIC number assigned by NCIC. LEADS does not assign a LID number to stolen vehicle entries.

If one or more of the fields in a wanted or missing persons record are not correct, you will receive a reject message listing the incorrect or required fields and a TID (Temporary Identification Number). The TID means your wanted or missing persons record has been placed in a temporary holding file until such time it can be modified and re-transmitted to the data files. Section 6 of this manual outlines the procedures for the temporary file records.

If you find it necessary to remove a screen format from your workstation, the shift and grave ( ` ) keys should be depressed.

### **3.14 WEATHER**

The weather file contains road and weather conditions for all areas of the state of Ohio. The Ohio Weather File is broken down into seven different areas of the state and aviation.

Weather information for Ohio is updated automatically with the National Weather Service Zone Weather Forecast four times daily. The weather information for segments of the state is updated by LEADS Control and the State Highway Patrol District Headquarters as conditions change. Updates by LEADS Control and the District Headquarters will be made at least twice daily from November 15 through April 1. Adverse local weather conditions should be reported to LEADS Control as they occur.

#### **3.14.1 HOW TO CONSTRUCT A MESSAGE**

The inquiry message record format consists of two parts: the message key code, and the area weather code. A period separates the message key from the area weather code. The following is a listing of the eight codes and corresponding areas you can inquire upon for Ohio:

<u>Code</u>	<u>Weather Area</u>
OH	Entire State
NE	Northeast Ohio
NW	Northwest Ohio
SE	Southeast Ohio
SW	Southwest Ohio
CO	Central Ohio
TP	Ohio Turnpike
AV	Aviation

The number of lines returned in the response will vary based on the weather and/or road conditions specific to the state area code used in the inquiry.

*Inquiry Example:* WE.OH (TRANSMIT)

### **3.14.1.1 Zone Forecast Inquiries**

There are five different zone broadcasts generated for the state of Ohio. The information in the broadcasts originate from the following locations:

- Z1 – Cleveland, Ohio
- Z2 – Pittsburgh, Pennsylvania
- Z3 – Charleston, West Virginia
- Z4 – Wilmington, Ohio
- Z5 – North Webster, Indiana

The zone broadcasts contain information for the counties designated with the number for the zone as shown in Figure 3-2.

To inquiry on a zone forecast, type WE. and then the zone for which you desire information, then transmit. *For example:* WE.Z1(Transmit)

When initiating an inquiry using the “OH” State Area Code, the response will include the latest update from all five zone broadcasts mentioned above.

### **3.14.2 Out-of State Weather Inquiries**

For weather inquiries to an NLETS state, enter the message key HQ followed by a period, and the two letter abbreviation for the state.

NOTE: Not every state has an automated weather response.

NLETS State Inquiry Example:       HQ.MN       (TRANSMIT)

The response you receive will be a report on the weather conditions for the entire state (this example shows the state of Minnesota).

### **3.14.3 WEATHER BROADCASTS**

In instances of certain severe weather broadcasts, LEADS will activate an audible alarm at the time the severe weather broadcast message is received from LEADS Control.

Severe Thunderstorm Warning  
Tornado Warning  
Flash Flood Warning

### **3.15 ROAD CONSTRUCTION INFORMATION**

Between April 2 and November 14 road construction which adversely affects travel by the motoring public will be entered in the LEADS Weather/Road file by OSHP District Headquarters. It is not the intent of the file to contain all construction zones in the state, but will include major construction zones impacting traffic.

1. The file will be updated by each OSHP district upon receipt of road construction information from OSHP posts.
2. The file will include:
  - a) Type of construction; i.e., repaving, bridge repair, reconstruction, etc.
  - b) Length of the construction zone.
  - c) Condition which is affecting traffic such as, lane closed; restricted lanes; bilateral in use; road closed completely. If a detour is being utilized, the route of the detour and its length will be included.
  - d) Hours and days of known or anticipated traffic slowdown and associated problems will also be noted. Duration of traffic delay will be included.
  - e) Only construction zones which will delay or adversely affect traffic for two (2) or more days will be entered. Primarily interstate, U.S., and state routes will be listed.

An exception to the two (2) day guideline may be a complete temporary road closing; i.e., chemical spills, landslides, etc.

Construction areas which continue to adversely affect traffic during the period November 15 through April 1 can remain in the file if space is available.

### **3.16 ORI MENU**

LEADS has installed a program on the workstation to assist operators in fulfilling the NCIC requirements to insert non-terminal ORIs in transactions run for those agencies. This program will allow the insertion of locally selected ORIs with either a combination of keystrokes **or** use of the mouse. Because the selection of these ORIs is an agency preference and subject to changes from time to time, the program is written to allow each agency to compile their own lists.

The use of non-terminal ORIs in transactions is required, but use of this ORI menu program is optional. The selection of ORIs, and the decision to use this program, is completely at the discretion of each terminal agency. Along with this flexibility comes the responsibility to update the chosen ORIs which also rests with the agency. This section of the Operating Manual outlines the steps to using this option.

If the agency chooses to use this program, the selection of ORIs to be used should be made prior to beginning the update process. The program allows for up to nine (9) Ohio ORIs. Agencies with more than nine non-terminal agencies should prioritize them based on the frequency of their use. Agencies with less than nine non-terminal agencies may consider using the program to input ORIs frequently contacted by administrative message. Any legitimate Ohio ORI can be entered and used with this program.

The setup process requires LEADS service be temporarily interrupted, so the time selected to perform the setup should be chosen with officer safety in mind. The agency TAC, while not required to perform the actual setup, should be involved in the setup process and will be responsible for training all operators in the use of the program.

#### **3.16.1 Menu Setup and Modifications**

1. Close the LEADS session;

*WITH THE MOUSE:*

Click on the minus or hyphen sign in the upper left corner of the screen above the word 'File' then click on 'Close'.

**OR**

*WITH THE KEYBOARD:*

Hold the 'Alt' key down while pressing 'F4' along the top of the keyboard (Alt + F4).

2. The UnixWare Desktop should now be displayed showing several icons. ***If it is, proceed to step three.*** Use the procedure in step 1 to close any open sessions other than the UnixWare Desktop. If all you see is an icon of a desk with 'UnixWareDeskt' in the lower left of the screen you need to restore it to full screen.

*WITH THE MOUSE:*

Click on the icon then select 'restore' from the menu

**OR**

*WITH THE KEYBOARD:*

Depress the Alt + F5 keys.

3. Locate the icon entitled 'UtsOriCfg'

*WITH THE MOUSE:*

If you need to move around the window to find this icon, position the mouse on the horizontal or vertical scroll bars on the bottom or right side of the window, click and *drag* the bar the direction you wish to move. You can also position the mouse on the arrows at the ends of the bar then press and hold the mouse button until the window is positioned properly.

**OR**

*WITH THE KEYBOARD:*

Use the arrow keys to move from icon to icon until the proper icon is visible. The selected icon will be highlighted to show you which is active.

4. Select the 'UtsOriCfg' icon

*WITH THE MOUSE:*

Double click (clicking the left mouse button twice quickly) on the icon. This will start the setup program. A blank window will flash on the screen before the menu window appears.

**OR**

*WITH THE KEYBOARD:*

Use the arrow keys to move to the 'UtsOriCfg' icon. You will need to use the mouse to activate this icon by double clicking (*see mouse directions*).

5. Enter the ORIs you have selected in the boxes titled F1 through F9. Any of the boxes may be used, and either upper or lower case may be used when typing in the ORIs.

*WITH THE MOUSE:*

Point to the box you wish to work with and click on the left mouse button. A large capital **I** will indicate the position of the cursor for typing. If you double click, the entry currently in the box will be highlighted. You can type over the highlighted text, or you need to backspace over the text you wish to replace. Type in the ORI you wish to be associated with the selected numbered box. Verify the entries, and make any corrections necessary.

**OR**

*WITH THE KEYBOARD:*

Use the tab key or up and down arrow keys to move to the box position you wish to work with. This method will highlight the text already in the box selected. You can type over the highlighted text, or you need to backspace over the text you wish to replace. Type in the ORI you wish to be related with the selected numbered box. Verify the entries, and make any corrections necessary.

6. Apply the updated information for the program to use in the future.

*WITH THE MOUSE:*

Click on the 'APPLY' button. This will end the menu window and return you to the UnixWare Desktop. Do not use 'Quit' because it will end the program without saving the new ORIs.

**OR**

*WITH THE KEYBOARD:*

Depress the Alt + A keys together. This will end the menu window and return you to the UnixWare Desktop.

***If an invalid ORI is entered in any of the boxes, the program will highlight the incorrect entry in red and prompt you to make corrections.***

7. Restart UnixWare Desktop software by closing the Desktop session. This is performed the same way it was for the LEADS session, but instead of 'Close' this menu uses 'Exit Desktop' (*see step 1*). The system asks you to verify your intention to exit. Choose 'Save Session and Exit' to make this verification.

*WITH THE MOUSE:*

Click on the 'Save and Exit' button. This will take you to the Novell Login screen *or a dollar sign*.

**OR**

*WITH THE KEYBOARD:*

Press the Alt + S keys together. This will take you to the Novell Login screen *or a dollar sign*.

**If you see a dollar sign type 'exit' and press enter to return to the Novell Login screen.**

8. Log in to the workstation with your login ID (i.e. dispatch) and your password (i.e. leads1). After a few seconds your LEADS session will return and the ORI menu program will be running. You should notice the addition of nine new icons across the top of the screen. These are shaped like the State of Ohio and are numbered 1 through 9 to correspond with the ORIs entered.

### **3.16.2 Use Of The ORI Menu**

The program displays your entries for all nine choices along the top of the screen, but the LEADS session window covers the list. To display the choices, adjust the size of the LEADS window. *Use of the mouse is required for this adjustment.*

1. Position the mouse pointer at the very top center of the screen. The mouse will change to an arrow pointing up to a line when in the correct position. Continue to move the mouse up until the mouse is on the top border and changes to the arrow pointing up to a line. When the mouse is positioned properly, press the left mouse button and hold it down while *dragging* the top border of the LEADS window down approximately 1 inch. The window itself will not change size until you release the button, but a shaded line will indicate the position while the adjustment is made. The window size can be adjusted up and down to your preference. Reducing it beyond the ORI menu will not serve any purpose, but it will result in less viewing space.

The active window is the window in which the computer is working. If more than one window is displayed, the active window may be distinguished by the colored title bar across the top of the window. To change active windows, place the mouse anywhere within the window you wish to work with, and click the left mouse button once. The title bar will change colors to indicate it is now active.

2. To enter an ORI form the menu into a LEADS transaction.

*WITH THE MOUSE:*

Begin the transaction as usual, then click on the numbered icon representing the desired ORI. The programmed ORI will be automatically placed at the location of the cursor followed by a period. The remainder of your LEADS transaction can then be entered and transmitted.

**OR**

*WITH THE KEYBOARD:*

Depress and hold the Shift + Ctrl + Alt keys and press the F1 through F9 key representing the ORI. The programmed ORI will be automatically placed at the location of the cursor followed by a period. The remainder of your LEADS transaction can then be entered and transmitted.

### 3.17 ESCAPED VIOLENT FELON NOTIFICATION SCREEN

Effective September 30, 1999 Ohio Revised Code Section 341.011(A), concerning the escape of a felon charged with an offense of violence, requires a county sheriff to notify all law enforcement agencies in their jurisdiction of an escaped felon from their custody. ORC Section 341.011(A) states a notification shall be sent when:

- 1) A person who was convicted of or pleaded guilty to an offense of violence that is a felony or
- 2) Was indicted or otherwise charged with the commission of an offense of violence that is a felony escapes from a county jail or workhouse or otherwise escapes from the custody of the sheriff of that county.

A LEADS formatted screen has been developed to assist in this process. Type in the message key EVFNOT . and transmit, the following screen will be returned:

```
EVFNOT.                ESCAPED VIOLENT FELON NOTIFICATION SCREEN

AGENCY/ (This defaults to your agency name.)
INCARCERATING FACILITY / _____
ESCAPEE: LAST /_____ FIRST /_____ MI /_ AGE /___
HGT /___ WGT /___ HAI /___ EYE /___ RAC /_ SEX /_

CLOTHING DESCRIPTION:

_____  

_____  

_____

NARRATIVE:

_____  

_____  

_____  

_____  

_____
```

