COMMISSION ON CRIMINAL AND JUVENILE JUSTICE

BUREAU OF CRIMINAL IDENTIFICATION'S CRIMINAL HISTORY FILE

AGREED-UPON PROCEDURES REPORT

FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

AUDIT REPORT NO. 93-23

TOM L. ALLEN, CPA
UTAH STATE AUDITOR

149103

COMMISSION ON CRIMINAL AND JUVENILE JUSTICE

BUREAU OF CRIMINAL IDENTIFICATION'S CRIMINAL HISTORY FILE

AGREED-UPON PROCEDURES REPORT

FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

AUDIT REPORT NO. 93-23

STATE OF UTAH
JAN. 4, 1896
STATE AUDITOR

TOM L. ALLEN, CPA
UTAH STATE AUDITOR

Tom L. Allen, CPA
STATE AUDITOR

STATE OF UTAH
Office of the State Auditor
211 STATE CAPITOL
SALT LAKE CITY, UTAH 84114
(801) 538-1025
FAX (801) 538-1383

DIRECTOR OF AUDIT
Auston G. Johnson, CPA

AUDIT MANAGERS
Joe Christensen, CPA
Dale Dillon, CPA, CISA
H. Dean Eborn, CPA
Stanley R. Godfrey, CPA
Jana R. Obray, CPA
John C. Reidhead, CPA

October 19, 1992

David Walsh, Acting Executive Director
and
Commission on Criminal & Juvenile Justice
101 State Capitol
Salt Lake City, Utah 84114

Dear Mr. Walsh:

At your request, we have applied certain agreed-upon procedures, as discussed below, to provide information on the quality of data in the Bureau of Criminal Identification's (BCI) Criminal History file. These agreed-upon procedures included the following:

a. We reviewed a sample of felony convictions from the Administrative Office of the Courts' computer system and evaluated how the information is transmitted to Bureau of Criminal Identification (BCI). We also reviewed the completeness, accuracy and timeliness of the information.

b. We investigated any sample items which lacked OTN numbers or for any other reason were not reported to BCI to try to determine the reasons the information is missing.

c. We reviewed items from the Courts' suspense files to try to determine why the items are in suspense, including what information is lacking and why.

d. We performed reviews of access, systems development and program change controls for both the Courts' and BCI's computer systems.

Our procedures performed for the limited purpose described in the first paragraph did not constitute an audit made in accordance with generally accepted auditing standards and would not necessarily disclose all material weaknesses in the systems. Accordingly, we do not express an opinion on the systems of internal controls taken as a whole.

This report is intended solely for the information and use of the Commission on Criminal and Juvenile Justice and is not to be used for any other purpose. This restriction is not intended to limit the distribution of this report which, upon acceptance by the Commission, is a matter of public record.

The accompanying findings and recommendations are based upon conditions noted during our review and are not intended to be all-inclusive.

We appreciate the courtesy and assistance extended to us by the personnel of the Commission of Criminal and Juvenile Justice, the Courts, and BCI during the course of our audit and we look forward to a continuing professional relationship. If you have any questions, please contact Dale Dillon, Information Systems Audit Manager, at 538-1351.

Tom Allen

October 19, 1992

UTAH STATE AUDITOR

BUREAU OF CRIMINAL IDENTIFICATION'S CRIMINAL HISTORY FILE

CRIMINAL HISTORY RECORDS SYSTEM

TABLE OF CONTENTS

CRIMINAL HISTORY RECORD SYSTEM
FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

Introduction

The Bureau of Criminal Identification (BCI) maintains the Utah Arrest and Filing/Disposition Reporting System (Criminal History System). The purpose of this system per the Utah Code (77-26-3) is to maintain information about individuals, "who have been arrested for or convicted of a crime under the laws of any state or nation... . The bureau shall make a complete and systematic record and index of the same." The purpose of our audit was to review the Criminal History System, determine the completeness and accuracy of the system, and determine why information is missing from the system.

For any system of information to be complete and accurate, controls must be in place to help guarantee that completeness and accuracy. Normally, these controls occur at the "boundary" of a system. The boundary is defined as the place where exchanges occur and information about the exchange is created. BCI wants to record both arrest information and disposition information on arrests. Therefore, in the Criminal History System, the boundary is when and where an individual is arrested and also when and where a disposition occurs. In the Criminal History System, multiple boundaries exist making the control over the information more complex and difficult.

Arrest information is collected at the jails during the booking process. However, an individual also can enter the criminal justice process by a summons and thus bypass booking. Therefore, the arrest information has multiple boundaries.

The boundaries for dispositions are even more complex. In most cases, dispositions are connected with the courts, but the disposition can take place at different steps in the court process or even external to the court process. For example, an individual can be arrested and then released without prosecution. In this case, the disposition would occur outside of the courts. To ensure that all arrest and disposition information is reported on the Criminal History System, completeness and accuracy controls must be in place at all boundaries where the arrests and dispositions occur.

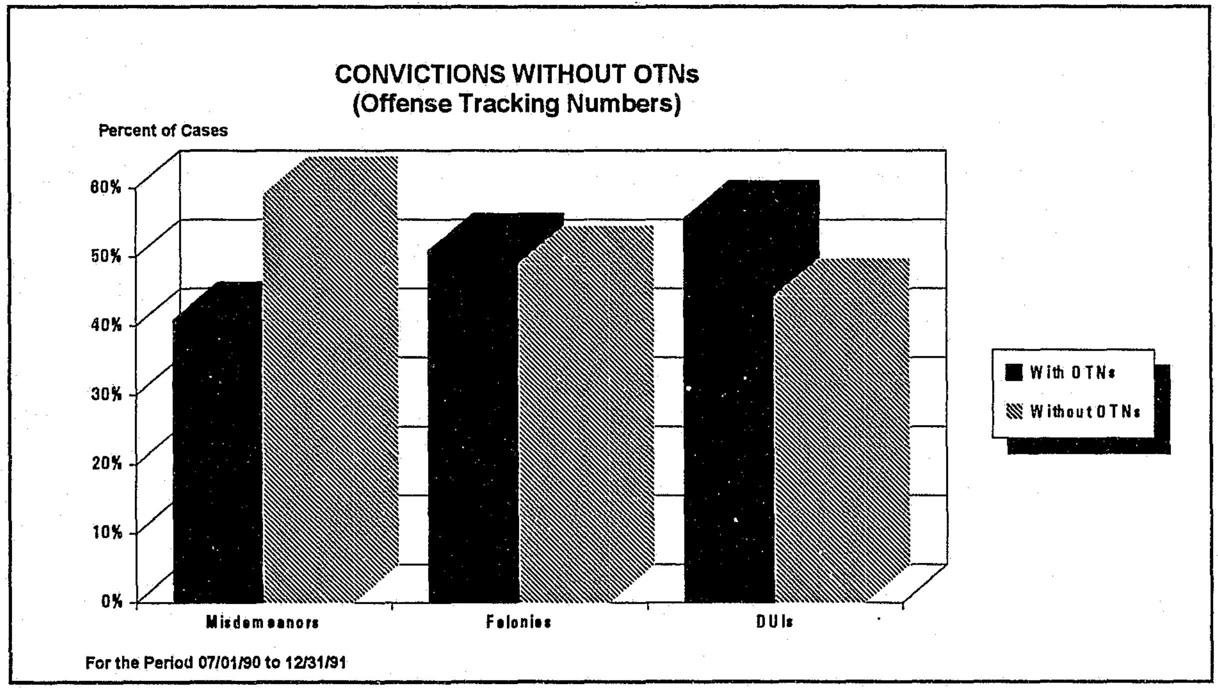
Methodology

As we discovered in our previous audit, the total population of arrests for a given period of time cannot be easily determined. The key to the Criminal History System is the Offense Tracking number (OTN) which BCI uses to trace individuals entering the criminal justice system. The OTN is part of the fingerprint card and initial arrest information and is pre-stamped on the form. When an individual is booked into jail, fingerprints are taken and the OTN on the form becomes the identifier for the arrest. The forms are distributed to arresting agencies, but no control is maintained over the forms. Therefore, we were unable to identify the total population of forms used for the time period we were testing.

CRIMINAL HISTORY RECORD SYSTEM
FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

As in our prior audit, we decided to select our sample from information on the Courts system. From the Administrative Office of the Courts, we obtained cases with convictions for July 1, 1990 to December 31, 1991 from both circuit and district courts. We totaled the number of cases and the number of cases without an OTN. (See Chart Below). Since dispositions without an OTN will have a difficult time being posted to the Criminal History System, this testwork gave us an indication of the percentage of disposition information missing from the Criminal History System.

Next, we took a random sample of dispositions, with and without OTNs. For the items with OTNs, we looked at the information on the Criminal History System to determine if the arrest information was recorded. For those sample items without OTNs, we went to the individual courts and investigated the cases to try and determine why the OTNs were missing. We then examined the information on BCI's system to determine if the sample cases were included on that system. We examined both arrest and disposition information for consistency and completeness with the Court system information. We followed these procedures for both a sample of felony cases and for a sample of DUI cases.


CONVICTIONS WITHOUT OTNs
(Offense Tracking Numbers)

For the Period 07/01/90 to 12/31/91

In addition to examining a sample of cases, we performed a general controls review on the computer systems for both the Courts and Public Safety which process and maintain data for the Criminal History System. General controls are procedures within the information systems department which ensure that the computer programs operate properly and that unauthorized changes are prevented. They include controls over the design, implementation, security, and use of computer programs and files. These controls consist of a combination of programmed and manual procedures. Improperly controlled computer environments can expose a system to improper functioning and can result in errors.

Conclusion

Our purpose in performing this audit was to determine the completeness and accuracy of the Criminal History System. Because of the weaknesses in the system discussed above, we could not statistically quantify our results. However, from our testwork, it is possible to conclude that the Criminal History System is substantially incomplete.

The chart above estimates the extent of the problem. Approximately 50% of all felony cases on the Courts System will not be included on the Criminal History System due to the lack of OTNs on those cases. Therefore, the Criminal History System is not a complete history of arrests and dispositions. Users should take this into consideration before placing reliance on it for such information.

It is impossible to determine the full impact that the lack of an accurate Criminal History System has upon the court and law enforcement systems in Utah. However, it is obvious that the risk of law enforcement agencies and courts making improper decisions increases significantly without an accurate history of criminal activity on individuals.

CRIMINAL HISTORY RECORD SYSTEM
FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

FINDINGS AND RECOMMENDATIONS

Findings

Based on the testwork described above, we had a number of findings concerning the Criminal History Record System and the process of obtaining information for that system. These findings are presented below.

1. Lack of Fingerprinting

The fingerprint cards used by the jails contain an Offense Tracking Number (OTN). The Bureau of Criminal Identification (BCI) uses this number to track individuals entering the criminal justice system. This number links arrests with dispositions and sentencing. We reviewed cases from 17 different Circuit or District Courts to determine the accuracy and completeness of the information on the BCI computer system.

Of 50 felony cases extracted from the Court's System, 27 did not have OTNs on the Court's system. In 8 of the 27 cases, the individual charged was not fingerprinted.

a. Of the 8 cases, 1 individual was booked into jail and 2 were arrested and released. However, the jails or police stations could not determine if the individuals had been fingerprinted.

b. For the remaining 5 individuals, the defendants appeared in court because of a summons. These individuals were not fingerprinted at arraignment, so an OTN was not generated. However, 1 of these individuals committed the offense while at the Utah State Prison. The charge for the case was listed under the custody screen of the OTN for the conviction that placed the individual in prison originally. Therefore, if the custody screens are not reviewed, this charge would not be detected when scanning the BCI file.

We recommend that the Courts make the OTN a required field on the Court data entry system. The OTN should contain a check digit to minimize the chances of incorrect entry. All OTNs should be checked against a table of existing OTNs for possible duplications. Also, procedures should be established to ensure that the charges and resolutions are properly recorded on BCI's system for crimes committed in prison.

We further recommend that all parties involved, including Courts, arresting agencies, and prosecutors, help ensure that including OTNs is a high priority.

Court's Response:

The OTN number is a very high priority item in the court data entry system. Due to the court delay that would result, it has been deemed unacceptable to withhold the filing of *cases when the OTN is missing. As your finding #2 indicates, there are a significant number of cases in which the OTN never reaches the proper court. If this problem could be corrected, it would become much easier to require the OTN at the time of filing. As it presently is constructed, the data entry system flashes warnings to the operator when an entry has been made without the OTN. The Courts have always supported the inclusion of a check digit in the OTN for validation purposes. This would reduce much of the error correction work which is caused by erroneous OTN numbers. We are quickly moving to a process in which the OTN will be sent to the court via computer from the Salt Lake County Attorney's Office. This will greatly reduce errors and omissions in the OTN number.*

Public Safety's Response:

A procedures has been established through the courts that when individuals receive a summons, it is indicated on the summons that the person is to go to the booking facility to be fingerprinted prior to appearing in court on the charges. The Office of the Court Administrator has a policy in place that requires a person to be fingerprinted prior to appearing before a judge. (Judicial Code Rule 4-609)

It is the understanding of Public Safety that the courts, through the Office of the Court Administrator, has made the OTN a mandatory field in their computer programs. However, it should be noted that Public Safety has programmed secondary field, i.e. Name, Date of Birth, Date of Arrest, as matching criteria when the OTN is missing.

Discussions are currently taking place with the courts on the process with the new Office Tracking form in developing a check digit as part of the Offense Tracking Number.

The Process is in place for the Utah State Prison to fingerprint individuals who have been charged with a crime while incarcerated at the Utah State Prison. This information will then be recorded on the criminal history files.

It should be noted that Public Safety has placed capturing the Offense Tracking Number a high priority, believing that if we receive the OTN we will capture all necessary Criminal History information.

Commission on Criminal & Juvenile Justice's Response:

We believe that the inability of the system to transfer the connecting OTN number (fingerprint Identification Mechanism) between the booking agency and the courts is our number one problem. We currently have two pilot projects underway to address our greatest challenge, to match all dispositions with the associated arrest information.

FINDINGS AND RECOMMENDATIONS

Salt Lake County Pilot Project 1:

Criminal History data is often lost very early in the process because the booking officials send the Offense Tracking Number (hence fingerprint Id) to the wrong court. To combat this problem, we will increase the role of prosecution in the criminal history process by changing the flow of criminal history forms. With the new system the booking agencies will send the OTN forms from the jails to each local county prosecutor. When the prosecutor receives this form he will: 1) Attach the form directly to the information and forward it to the appropriate court with the arrest charges; or 2) the prosecutor will send the Bureau of Criminal Identification a copy of the form with new charges attached and then forward the amended form with the "information" to the correct court or 3) He will use the same form to submit the declination directly to the BCI.

Salt Lake County Pilot Project 2:

The shear volume in four counties (Salt Lake, Weber, Utah and Davis) makes implementation of a continual manual process of sending forms between jails and prosecution very difficult. To alleviate this, we are proposing an automated filing procedure. Under this plan the prosecutor will electronically receive the data from the jails and will then submit the filing form with the associated OTN number directly to the court.

2. <u>Control of OTN Forms</u>

Of 50 felony cases examined, 27 cases did not have OTNs. In 19 of the 27 cases, the arresting agency completed the OTN card, but the OTN was not recorded on the Court's System.

a. For 4 of the 19 cases, the arresting agency sent the OTN forms to the incorrect court and therefore, the OTN was not entered with the proper case on the Court's System.

b. For 13 of the 19 cases, the arresting agency did not send the OTN forms to any court, and therefore, the OTN was not entered with the proper case on the Court's System.

c. For 2 of the 19 cases, the OTN forms were received by the proper court, but not input into the Court's System.

Of these 19 cases which did have OTN cards, BCI captured arrest information for 17 of the cases. However, BCI did not receive dispositions on 13 of these 17 cases. The arrest information for 2 of the 19 cases was not captured on the BCI system.

We recommend that once fingerprints have been taken and an OTN associated with a case that the jails and courts establish a system to maintain and account for these forms to ensure that the information is transferred to the proper court in an accurate and timely manner.

Court's Response:

Control of the OTN forms is more complex than a simple jail/courts monitoring process. The prosecutors both city, county and BCI are integral to the flow of OTN numbers through the system. As your introductory statement indicates "In the Criminal History System, multiple boundaries exist making the control over the information more complex and difficult." Adequate control over the OTN cannot be accomplished unless it becomes a priority for more than just jails and courts.

Public Safety's Response:

BCI has developed a P.C. computer program, that when an agency requests OTN forms from BCI for fingerprinting, BCI records the OTN's on the computer, and as those forms begin to be returned, BCI can record them as received. In addition, BCI has printed the fingerprint box portion of the OTN form the back of the form. If an officer needs to reprint a person, the officer can turn the form over rather than use a new form. This helps in controlling the OTN forms. BCI has also established a process whereby an agency is to return all discarded OTN forms in order to account for all unused numbers.

Commission's Response:

We are proposing an automated procedure to receive arrest information from each county. As an integral part of this procedure we will collect booking numbers from the participating groups. While this will not directly address missing OTN forms, we believe the "breaks" or gaps in the booking numbers from each county will assist us in finding missing arrest information.

3. Accuracy of Information on BCI's System

Of the 50 felony cases tested, 23 cases had OTNs on the Court System. Of those 23 cases, BCI's system accurately recorded the charges and dispositions for 14 cases. For 5 of the remaining 9 cases, there appears to be a discrepancy between the charges and dispositions recorded on the Court's system and BCI's system. For 3 of the cases, the arrest information was captured, but there were no dispositions listed on the BCI system. For the remaining case, the disposition on the Court System appeared to be different than the disposition on the BCI system.

We recommend that a quality control process be established to compare Court System information to the information on the BCI system to help ensure accuracy of the charges and dispositions on BCI's system.

Court's Response:

There is an increasing need to improve the cooperation between BCI and the courts. This recommendation should go beyond a simple compare of information to include consistency of data formats and codes. This would make quality control and comparisons much easier to analyze and compare. It would also reduce the rate at which errors occur since we are always translating codes between the two agencies.

Public Safety's Response:

We concur that there should be a quality control process comparing court data to information on the Utah Criminal History files. Currently BCI receives a magnetic tape containing disposition data from the Office of the Court Administrator. This tape is run against the Utah criminal history files to match court disposition with arrest. When the disposition information does not match an arrest, the disposition information goes into a suspense file and a computer printout is generated. The computer printout is then used to manually match the court disposition to arrest on the Utah Criminal History files.

4. Timely Receipt and Processing of OTN Forms

Courts input OTNs for cases when the court receives the OTN forms from the arresting agency. We found that some courts were receiving the OTN forms from arresting agencies approximately every two to three months. At the time of inquiry, one court indicated that at least three months had elapsed since the court had received OTN forms from an arresting agency.

We also found an instance where a Circuit Court's file contained an OTN form which had been received by the circuit court after the case had been bound over to the district court. Because of the timing problem, the OTN was never tied to that case.

We recommend that arresting agencies and courts ensure that applicable clerks are aware of the procedures for forwarding OTN forms to the appropriate court and that they send the forms to Courts and BCI on a timely basis. We also recommend that the Courts establish a policy for controlling late OTN forms so they can attach them to the appropriate cases on the Court's System.

Court's Response:

We agree with this recommendation. A procedure for controlling late OTN forms could be implemented and established in our clerical training programs. In addition, the courts are seeking to eliminate many of the timing problems by moving the information via computers wherever possible.

Public Safety's Response:

We agree that all appropriate agencies and people are made aware of the procedures in processing arrest and disposition information. BCI has developed an "Arrest and Disposition Reporting" manual which outlines all appropriate procedures. In addition we have a program specialist position dedicated to arrest and disposition reporting. This position works with local law enforcement prosecutors, courts and corrections to assure that information is processed completely, accurately and in a timely manner.

5. Use of DUI Citation Numbers

For DUI violations, the arresting officer will issue a citation to the offender. The citation number is used as the OTN. We reviewed 10 DUI cases from 6 different Circuit or District Courts to determine the accuracy and completeness of the information on the BCI system.

Of 10 DUI cases tested from the Court's system, 7 did not have citation numbers. When these 7 cases were reviewed on BCI's system, we found that 2 of the 7 cases were not on the BCI system. For 4 of the 7 cases, the charges were captured correctly onto the BCI system but the disposition data was blank.

For 1 of the 7 cases, the citation information was not recorded on the BCI system. However, an OTN was found which corresponded with the data in the case. It was determined that this was a commitment record. The individual was fingerprinted when she served her time in jail. Therefore, if this person had not been sentenced to jail, it is unlikely that the DUI violation would have been recorded on the BCI system.

Of the 3 cases which had citation numbers associated with the case, the charges and dispositions were captured accurately on the BCI system.

We recommend that a review or quality control process be established to compare court information to the information on the BCI system to ensure accuracy of the charges and dispositions. Also, formal procedures should be established to ensure that citation forms are sent to BCI and the correct court.

Court's Response:

We agree with this recommendation. Several problems have been discovered relating to the capture of citation numbers. Resolution of this problem will be integrated with Recommendation #3.

Public Safety's Response:

We concur that there should be quality control processes established to compare court information with the Utah Criminal History files. We believe that BCI has established quality control processes for accuracy as well as completeness of arrest and disposition data. (see #3)

6. Duplicate OTN Forms

Through inquiry and observation, we found cases where arresting agencies can assign multiple OTNs to the same incident. When an individual is booked on the city level, the arresting agency completes an OTN form. If the same individual is booked on the county level, the arresting agency completes another OTN form for the same case. The court has been entering whichever OTN it receives first. Therefore, BCI may be unable to close a case on their system because the OTN does not match the court reporting system.

We recommend that the Courts, arresting agencies, and BCI work together to help eliminate this problem and ensure the use of only one OTN form and number.

Court's Response:

We agree with this recommendation and suggest that the Commission on Criminal and Juvenile Justice assist in developing the method in which this can occur.

Public Safety's Response:

We agree that the courts, arresting agencies, corrections and BCI need to continue to work together to eliminate the problems of reporting criminal history information.

The Department of Public Safety through BCI has received nearly $500,000 in federal grants to rewrite the Utah Criminal History files and work on resolving the problems associated with reporting criminal history information to BCI. We believe that many of the problems are solved as stated above, however there is still work to be done, that is why BCI has dedicated a full time position to this task.

FINDINGS AND RECOMMENDATIONS

The following findings and recommendations pertain to the Administrative Office of the Courts computer system.

7. Lack of Control of Computer Access to Court Data

The Court Administrator's Office (Courts) does not have a formal policy for approving and granting user access privileges to Case Management System computer files. Unauthorized access to the Case Management System files could result in intentional or unintentional alteration of data. To ensure that only valid persons access the computer system, Courts should establish a security policy which includes a request form to document user access requests and management approval. The security policy also should include a procedure to immediately remove user access for employees who have been terminated or transferred to another position. If a transferred employee requires access for his new position, Courts should grant access after following the procedures prescribed above. The request forms should be maintained in an accessible manner which will confirm an individual is authorized to access the computer system.

We recommend that the Courts establish a formal security policy to be followed to grant and remove user access privileges for the Court's Case Management computer system.

Court's Response:

We are in agreement with the findings concerning the computer center and the security procedures. Some of the specific recommendations made in this portion of the report have become irrelevant since we are in the process of replacing our Wang computer system. These recommendations do, however, form an excellent framework around which we will establish security for our future system. All of the concepts identified in the report will be brought forward into the new computer system with the exception of Recommendation #12, which relates specifically to the Wang environment and is not relevant to the new system.

8. Excessive Security Administrator Rights on the Court's Wang Computer

Security administrator rights are granted to users other than the Courts' security administrators. Security administrator rights allow an individual to read, write, copy and delete all files, create new security administrators, and modify system security settings and user privileges. Because security administrator rights are so powerful, they should be limited and controlled to help ensure the integrity of the computer system and data.

All computer operators have security administrator rights through a generic computer access ID. This ID should be restricted by creating menu driven access which will only allow the operators to perform the functions needed to complete their duties.

All personnel in Data Processing (DP) operations have security administrator rights at all court sites either through an individual ID or by the use of a generic operations ID. Additionally, security administrator rights have been granted to WANG service personnel. These non-state employees can remotely access the Court's WANG(s) at anytime and make changes to the computer system. Users should be restricted to the minimum rights required to perform their functions.

We recommend that Courts only grant security administrator rights to the Courts' security administrators. When possible, alternative methods to complete work functions should be utilized for those who currently have excessive security rights. If security administrator rights are needed to perform a particular function or solve a problem, Courts should limit and grant the rights on an as needed basis after receiving management's formal approval.

Court's Response:

See response to recommendation #7 above.

9. Excessive Security Administrators on the Court's WANG Computer

Security administrator status has been granted to users other than the designated security administrator for each court. Generally, a security administrator is assigned at the court level and also at the Court Administrator's Office. However, both persons can and do add new users. No central responsibility exists to add, delete, or update users on the system. Security administrators can read, write, copy and delete all files, create new security administrators, and modify system security settings and user privileges. We reviewed the access privileges at the Salt Lake Circuit and Salt Lake District courts. Twelve users at the District and twenty users at the Circuit courts have been granted rights in excess of what is needed to perform their duties. No documentation exists from management authorizing that such rights are required.

Several of the Security Administrator IDs are group logons. Therefore, anyone knowing the password could have access to anything on the system.

If some security rights are needed to perform a job function, an ID can be created which will restrict access to the functions needed to complete the required duties. Security administrator rights have also been granted to two non-state employees which will allow remote access from any WANG. To ensure the integrity of the court system, if a user is required to have security administrator rights, Courts should restrict the functions to the minimum required to perform the tasks.

We recommend that Courts review all of the court's access privileges and only grant security administrator rights to the designated security administrators. When possible, Courts should utilize alternative methods to complete work functions for those who currently have excessive security rights. If security administrator rights are needed to perform a particular function or solve a problem, Courts should grant and limit the rights on an as needed basis after formal approval is received from management.

Court's Response:

See response to recommendation #7 above.

10. **Excessive User Options on the Case Management System**

The Case Management system has several user access IDs which are for inquiry of the Court's database. However, the access privilege for these Ids are set to 'write' instead of 'read-only'. Several of these IDs are group IDs, so anyone with knowledge of the password can alter the data. To ensure the integrity of the data, Courts should grant access at the lowest level that will allow the user to perform his duties.

Additionally, many users have operator status. Operator status allows users to print special forms. However, operator status also allows individuals to cancel jobs, load data (tapes), debug programs, logon remotely, and manage system tasks. If all users are required to print special forms, a menu should be created which will limit the operator functions that the users can execute.

We recommend that the Courts restrict users requiring inquiry to the Case Management system to 'read-only' access. We also recommend that the Courts restrict operator privileges to those performing operator functions. This will help ensure the integrity of the Case Management system data.

Court's Response:

See response to recommendation #7 above.

11. **Obsolete Logon IDs**

We tested 42 user access logon IDs for the Salt Lake District Court. 2 users of the 42 tested could not be found on the employee history file. To prevent unauthorized access to the Case Management system, the security administrator should remove all obsolete IDs immediately upon an employee's dismissal and/or when the ID is no longer required.

We recommend that the Courts remove all obsolete IDs on a timely basis to prevent unauthorized access to systems and data.

Court's Response:

See response to recommendation #7 above.

12. Lack of Documentation of WANG Computer Access Privileges

The WANG computer system grants access according to access privilege settings. These settings are defined as access groups A through Z. The Case Management system is located on Group C. Several users have access to groups other than C. However, the applications in the other groups are not documented, and it is not known whether users need this access to perform their job functions.

We recommend that Courts document applications and data located under the Access groups A, B, and D-Z so that access privilege settings can be properly controlled.

Court's Response:

See response to recommendation #7 above.

13. Weaknesses in System Development and Program Change Controls

During our review of system development and program change controls for the Courts Wang computer system, we found the following control risks:

a. Each program change is assigned a task number which will correspond to a release of the Case Management System which is run on the Court's Wang computers. Each task is assigned to a release based on priority. If a programmer decides a task will not be performed, he deletes the task which leaves gaps in the task numbering system. To ensure that all tasks are completed as prescribed, programmers should account for all task numbers. This would include a listing of the tasks that are currently not assigned to an analyst and those tasks which will not be completed.

b. The programming staff and the user group do not document testing for new programs or program changes nor do they formally sign-off indicating that tests were performed. A summarization indicating what tests were performed and the criteria for the test transactions used should be retained. Additionally, a formal sign-off would indicate that the testing has been completed and that the programmer and the user group are confirming that the changes to the program are proper.

c. A Site Transfer form is used to move new or updated programs into the production environment. The DP Director and the user group do not document authorization of program moves to the production environment, which would signify that the changes to the program are satisfactory. Additionally, the Site Transfer forms for the last four releases could not be located.

d. Generally, DP Operations moves new versions of the Case Management System to production on the Courts' Wang computers. However, all DP personnel have the ability to move programs into production. Adequate segregation of duties requires that the programming function be separated from the role of moving programs into production.

We recommend that Courts ensure that the task listing accounts for all tasks, including those tasks which will not be completed. We also recommend that the DP staff and the user group document that program testing was completed. The DP staff and the user group should retain a summarization of the tests performed with the criteria for the test data used. Both the DP Director and the user group should approve the Site Transfer request and these should be maintained in an accessible manner. Additionally, Courts should ensure that the programming function is separated from the responsibility of moving programs to production.

Court's Response:

See response to recommendation #7 above.

14. Lack of Contingency Plan

The Court Administrator's Office does not have a contingency plan in the event that computer services are disrupted. The plan should include a description of critical computerized systems and a formal plan for restoration or for alternate implementation of services in the event of an interruption. Additionally, only Salt Lake District and Salt Lake Circuit courts store backup data off-site. In the event that a disaster should occur, other courts could have to reconstruct data from source documents.

We recommend that the Courts develop and test a formal contingency plan. The plan should be comprehensive, covering all types and degrees of contingencies from illness of staff to destruction of the computer facility. We also recommend that the individual courts maintain off-site backup data.

Court's Response:

See response to recommendation #7 above.

15. Lack of Procedures for Handling and Disposal of Media

The Court Administrator's Office does not have formal procedures which instruct individual courts on the proper handling of the hardware and magnetic media which are located at the courts. Generally, each court has its own WANG system. Backup tapes are stored on-site. We toured 12 computer rooms and determined that several of the computers were not physically secured from public access. We noticed books and office supplies stacked on top of several computers. Many of the computers did not have a dedicated power supply or power surge protection. Not all computers were located in a temperature controlled environment to protect against heat and/or damage. Additionally, fire protection was limited to a few courts with fire extinguishers. Most clerks were uncertain of the procedures in case of fire or other emergencies. To reduce the likelihood of physical or magnetic damage, formal policies should be established to instruct the courts in the proper handling of hardware and magnetic media, including emergency procedures.

Additionally, there are no procedures for the proper disposal of sensitive media. A policy should include procedures for shredding sensitive printouts and the removal of data and software from hard disks, diskettes, and magnetic tapes.

We recommend that Courts establish policies and procedures to instruct the individual courts on the proper handling of hardware and magnetic media including emergency procedures and the proper method of disposing of sensitive material.

Court's Response:

See response to recommendation #7 above.

16. Lack of Quality Control Reviews

The courts do not verify that changes to the transaction and master files are correct. Changes can be verified through quality control reviews in which the supervisor could randomly compare case files to the court system to ensure that the data on the court system is accurate. These reviews should be documented and performed on a regular basis.

We recommend that the Courts establish a policy to perform quality control reviews on a timely basis to ensure the accuracy of the court system.

Court's Response:

See response to recommendation #7 above.

17. **No Background Checks on Employees**

The Data Processing section of the Court Administrator's Office does not perform background investigations before hiring new personnel. To ensure the integrity of the system and the data, background investigations should be performed before hiring personnel.

We recommend that the Courts establish and implement a policy to review the backgrounds of individuals applying for employment with Data Processing.

Court's Response:

See response to recommendation #7 above.

18. **Lack of Separation of Duties**

Clerks perform data entry at each court. However, for some of the smaller courts, the Court Administrator's Data Processing department performs the data entry. To maintain an adequate segregation of duties, data input should be separated from systems software programming, application programming and computer operations.

We recommend that someone whose job functions do not include systems software programming, application programming, or computer operations perform data input for the courts.

Court's Response:

See response to recommendation #7 above.

FINDINGS AND RECOMMENDATIONS

The following findings and recommendations pertain to the Department of Public Safety's computer system.

19. Excessive Access Privileges for Bureau of Criminal Identification (BCI) System

Three Public Safety Data Processing (DP) programmers have the ability to update the BCI database, write programs, and move programs into production. To adequately segregate duties, an agency should separate the programming function from the input and database update functions. This reduces the likelihood that an individual could change a program to accept fraudulent input supplied by that individual. Also, the agency should not permit programmers to move test programs into production as this has the potential for circumventing review and control procedures.

In addition to the 3 Public Safety employees noted above, 2 consultants have the same ability to update the database and write programs.

To help ensure the security and integrity of the database, Public Safety should restrict their programmers' ability to move test programs into production and the programmers' ability to input to and update the database.

Public Safety's Response:

We understand and concur with your recommendation to restrict the ability of programmers to move programs into production, etc., in the Natural environment. We are taking actions to restrict full access to only two individuals on a regular basis. Again, if an individual is gone for an extended time, we will authorize a substitute in order to maintain proper backup.

You also recommend that the person responsible for security be separate or segregated from programming duties. Unfortunately, we are so short of staff that it is not possible for us to dedicate a person strictly for security purposes. We have in the past, and are now requesting authorization and funding for a security specialist position, but do not currently have funds available.

While we do maintain the ability to move our Natural programs into production, you should be aware that the majority of programs in the Criminal History System are written in COBOL/CICS. This includes all programs that update the database. For this environment, only the security staff of the Division of Information Technology have the ability to move programs from test into production. Hence, for our COBOL/CICS programs we have both segregation of duties and restricted access for program moves.

20. Logical Access to BCI

Of 10 user IDs tested, 4 did not have an access request or other documentation which indicated that access to the system was authorized. Additionally, the requests for access that were found were several years old and in most cases did not have an authorizing signature. To ensure that only valid persons access the system, a request for access should include a request form to document the date of the request; the supervisor authorizing the request, the name, title, and phone number of the person receiving the access privileges, the access privileges being added, changed, or deleted; and the signatures of the employee, the employee's supervisor, and the Security Administrator. The access rights granted should be limited to allow the employee only to perform his job functions. Unauthorized access to the BCI System files could result in intentional or unintentional alteration of data. The request forms should be maintained in an accessible manner which will confirm the authorization of access to the computer system.

We recommend that Public Safety adequately document user access privileges and authorization to the BCI system.

Public Safety's Response:

A list of persons requiring access to the NATURAL library for the Criminal History system was sent to ITS in March of 1992, and revised list in May 1992. For some reason, the list in May was not applied. However, we are again revising the list and will re-submit to ITS.

We have also created an "access authorization" form for future access modifications to the UCCH NATURAL library. This form will be filled out by BCI and MIS and sent to ITS to be kept in a file for reference purposes. (see attached form)

We requested authorization and funding for a security specialist position in the last two budget cycles but were unsuccessful. We will be requesting a security specialist in the upcoming budget cycle in order that we can address your concerns which are a high priority of Public Safety. I assure you that we are doing the best we can to provide appropriate controls for this very important application.

21. Contingency Planning

Public Safety does not have a completed contingency plan for use in the event that computer services are disrupted. The plan should include a description of critical computerized systems and a formal plan for restoration or for alternate implementation of services in the event of an interruption.

CRIMINAL HISTORY RECORD SYSTEM
FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

FINDINGS AND RECOMMENDATIONS

We recommend that Public Safety develop and test a formal contingency plan. The plan should be comprehensive, covering all types and degrees of contingencies from illness of staff to destruction of the computer facility.

Public Safety's Response:

Public Safety recognizes the importance of contingency planning. Our Information Technology Plan starting on page 19 and running through page 21 addresses the activities we are presently involved in to move this ahead. Again, we are seeking a dedicated security specialist to complete our contingency planning in a timely fashion and at a standard that is required for the very sensitive and critical applications that Public Safety supports.

It should be noted that the most critical applications are located on the State's central mainframe. Therefore, a key component to our contingency planning is really one that needs to be addressed by Information Technology Services within the Administrative Services Department of the State.. Public.Safety will work closely with ITS in completing those portions of Public Safety Contingency Planning.

*Your recommendation suggests the plan should be comprehensive covering **all types and degrees** of contingencies from illness of staff to destruction of computer facility. A contingency plan that covers **all types and degrees** of contingencies would be extremely time consuming and, in my view, would not be in the best interest of the State. We recognize that we need to have a robust contingency plan addressing various levels, but we certainly cannot address **all types and degrees** of contingencies.*

CRIMINAL HISTORY RECORD SYSTEMS
FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

STATUS OF RECOMMENDATIONS IN THE 1990 REPORT

This section reports follow-up action taken by management on recommendations made in our prior report issued for the year ended June 30, 1990. The prior recommendations which have not been implemented, but are considered significant, have been repeated in our current report.

1. Timely Receipt of Computer Tapes From Courts

We recommend that the Courts send updates to BCI at least monthly as required by statute. Also, if the Courts need to modify systems in the future, they should plan to continue providing information to BCI during all phases of the systems development or change process.

Status:

Implemented.

2. Coordinating Coding for Criminal Offenses

We recommend that the Legislature establish by statue a uniform set of legal codes and law enforcement agency abbreviations that courts can use. In coordination with BCI, the Courts should then ensure that these codes are accurately translated between the Courts' system and BCI's Criminal History System.

Status:

Implemented. Although not done through legislation, there is a centralized controlling of codes through the uniform bail schedule. This includes the centralization and control of local legal code violations and law enforcement abbreviations.

3. Communication of CDR Numbers

We recommend that the Courts make the CDR number (Court Disposition Record, now called Offense Tracking Number -OTN) a required field on Court data entry systems. Also, the CDR number should contain a check digit to prevent incorrect entry and all CDR numbers should be checked against a table of exiting CDRs for possible duplications.

We also recommend that Pre-trial Services, because of the proximity to the booking process, have responsibility for obtaining the court's copy of the CDR form and transferring the number to the Pre-trial Services worksheet which is sent to the circuit courts.

Status:

Not implemented. See current recommendation No. 1.
As of March, 1992, the prosecutors have taken additional responsibility to help ensure that OTNs are connected with Court cases and that if an OTN does not exist that the arrested individual will be fingerprinted.

CRIMINAL HISTORY RECORD SYSTEMS
FOR THE PERIOD JULY 1, 1990 TO DECEMBER 31, 1991

STATUS OF RECOMMENDATIONS IN THE 1990 REPORT

4. **Tracking CDR Number When Additional Charges Are Filed**

   We recommend that the Courts establish a method to link the CDR number from the original arrest and case to any other cases that may result from additional charges being filed in conjunction with the arrest.

   Status:
   Problem not noted as part of this audit.

5. **CDR Numbers in Cases Started With a Summons or Citation**

   We recommend that the Legislature clarify which agency is responsible for the actual fingerprinting of those convicted of criminal offenses. This agency should have the facilities and personnel trained to perform this duty.

   Status:
   Partially implemented. Information noted by involved agencies. Finding not repeated.

6. **Completion of Fingerprint Cards**

   We recommend that BCI account for all CDR forms by requiring law enforcement agencies to return both completed and voided CDR fingerprint cards. If the agency cannot return the card for any reason, they should notify BCI of the number and disposition.

   Status:
   Not implemented. See current recommendation No. 2.

7. **Suspense file on BCI Criminal History System**

   We recommend that BCI revise the Criminal History System to include an error suspense file. A suspense file will allow BCI to control unmatched records so they can be re-entered into the system or subsequently investigated.

   Status:
   Implemented.

8. **Completeness of Records Reported from the Courts to BCI**

   We recommend that the Courts run a separate report to gather items with a CDR number, judgement code, and date which have not been reported and forward this information to BCI.

STATUS OF RECOMMENDATIONS IN THE 1990 REPORT

Status:

Implemented. With the new BCI system, the Courts no longer hold cases in their system. Items are sent to BCI after a certain time period and would be captured in BCI's suspense files if no match occurs.

9. **Other Observations**

a. BCI should consider rewriting the Criminal History System

Status:

Implemented.

b. An arrest-based criminal history system such as Utah's, requires cooperation from all agencies involved. Most data-contributing agencies, as indicated by their actions, place low priority on this System.

Status:

Information noted by involved agencies. Finding not repeated.

c. The Commission on Criminal and Juvenile Justice is ultimately responsible to assure that any criminal history system is complete and accurate. They must provide BCI the authority to enforce the collection of data.

Status:

Information noted by involved agencies. Finding not repeated.

d. Our review of the Criminal History System showed that BCI also stores information on noncriminals such as security guards as part of their files. Because of the condition of the files and difficulty in maintaining the programming, placing anyone on the Criminal History System other than those persons outlined by the Utah Code has the potential for misleading users of the system.

Status:

Implemented.