A PRIVACY AND SECURITY AUDIT OF THE ALASKA JUSTICE INFORMATION SYSTEM

September 1978

By: F. Kaye Tomlin
Senior Research Engineer
Information Science Laboratory

Prepared for:

State of Alaska
Office of the Governor
Criminal Justice Planning Agency
Juneau, Alaska

SRI International
333 Ravenswood Avenue
Menlo Park, California 94025
(415) 326-6200
Cable: SRI INTL MNP
TWX: 910-373-1246

A PRIVACY AND SECURITY AUDIT OF THE ALASKA JUSTICE INFORMATION SYSTEM

September 1978

By: F. Kaye Tomlin
Senior Research Engineer
Information Science Laboratory

Prepared for:

State of Alaska
Office of the Governor
Criminal Justice Planning Agency
Juneau, Alaska

SRI Project 7599

Prepared under Grant Number 76-A-039, awarded to the State of Alaska Criminal Justice Planning Agency by the Law Enforcement Assistance Administration, U.S. Department of Justice.

CONTENTS

TABLE

I EXECUTIVE SUMMARY

Summary of Findings and Conclusions

Based primarily on the results of a 5-day visit to Alaska between June 12, 1978 and June 16, 1978, this report describes the deficiencies observed and the recommendations that should be considered in addressing the improvement of the Alaska Justice Information System (AJIS) privacy and security.

Although a number of deficiencies were noted during the course of the visit, this report has used them as the basis for one broad and overriding primary recommendation and has separated the discussion between the specific deficiencies and the overview perspective.

The major deficiency is that no AJIS privacy and security management program exists, and, as a result, privacy and security performance has been seriously affected. We believe that, with the implementation of such a program, the performance will be quickly and dramatically enhanced. Specifically, in our primary recommendation we have suggested:

- Development of an AJIS Policy and Procedure Manual that addresses privacy and security guidelines, standards, policies, and procedures as they apply to individuals and facilities that constitute or come in contact with AJIS.
- Establishment of a mechanism by which privacy and security problems can be rapidly identified and resolved, with the authority to be held initially by the AJIS Committee that was established recently by the Governor's Commission on the Administration of Justice (GCAJ).
- Dedication of the AJIS Security Officer on a full-time basis to privacy and security matters, including a training function, along with sufficient resources to adequately support these duties (this position could be renamed the AJIS Security and Training Officer).
- Assignment to the full-time AJIS Security Officer of the responsibility for day-to-day enforcement and training in privacy and security matters.

- Assignment of responsibility to the AJIS Committee for addressing and resolving the specific deficiencies described in this report.

It should be noted that this report has concentrated on deficiencies as opposed to the more positive aspects of AJIS security. Indeed, there were some excellent examples of security observed, notably in the data processing environment and scattered user sites. The quality of privacy and security was mostly a function of the individuals at the sites and their awareness and efforts without the benefit of any specific and continuing guidance. It is the individuals at the sites on whom the security performance will depend in the future, and, if the sites visited during this audit were any indication of all AJIS sites, there is a generally good foundation on which to build.

Report Organization

Following this Executive Summary is an introductory section that provides the project background and audit methodology. Section III presents the major finding and recommendation, and Section IV the specific deficiencies and their associated recommendations. Supporting information is provided in a schedule of site visits (Appendix A) and the interview form that was developed for this audit (Appendix B).

II INTRODUCTION

Background

This report documents the observations and recommendations of a privacy and security (P&S) audit of the Alaska Justice Information System (AJIS) performed by SRI International under contract to the State of Alaska's Criminal Justice Planning Agency (CJPA). The goal of the audit was to evaluate the conformance of AJIS, its users, and its user sites to certain aspects of the applicable state statutes* and regulations,† as well as to the State of Alaska Privacy and Security (P&S) Plan of December 1975. Specifically, SRI was directed to concentrate on three major aspects: Personnel Selection, Physical Security, and Individual Right of Access.

The audit is one of two tasks in a larger project that also has an objective to assess the status of AJIS operational and technical accomplishments. The work of the other task will include: collection of relevant data (e.g., overall goals, system implementation costs, current operating costs, system statistical performance data, and system configuration); development of a description of the current system; comparison of goals with accomplishments; and the preparation of an assessment report that will include findings, conclusions, and recommendations. Although this audit report is being published separately, the two documents necessarily will be closely related--the overall system performance obviously affects the P&S performance of its users.

---

*Chapter 62, Criminal Justice Information Systems Security and Privacy, October 1, 1972.

†Title 6, Part 3 (Governor's Commission on the Administration of Justice), Chapter 60 (Criminal Justice Information Systems), Articles 1 through 5, Register 45, April 1973.

Methodology

The first steps in the audit process involved review of applicable AJIS documents and the subsequent preparation of an interview form and a site visit schedule. Coordination with CJPA staff resulted in the determination of the three audit areas to be covered (Personnel Selection, Physical Security, and the Individual Right of Access) and a site visit schedule. The interview form, shown in Appendix B, was developed using CJPA guidance, the P&S plan, and interview forms developed by SRI for similar work. A rating guide was included in the form. The site visit schedule was finalized as the trip was in progress, with the final schedule as shown in Appendix A. The interview form is specifically included in this report for potential use by the AJIS Security Officer and future audits.

During the course of the 5-day trip, 19 sites were visited (one during an unannounced, spontaneous visit) in Anchorage, Juneau, and Ketchikan, and interviews were conducted with the AJIS Security Officer (ASO), the AJIS Director (AD), Terminal Security Officers (TSOs), Terminal Operators (TOs), and site supervisory personnel. The interviews were conducted to solicit user knowledge of AJIS security practices and to provide an evaluation of the security performance for each site, for AJIS as an entity, and for the two major functional areas: system users and system support functions (i.e., the AJIS security program and the data processing aspects). Furthermore, the audit was to be performed by evaluating user and support conformance to the three chosen areas as specified in the P&S Plan and then assigning a subjective rating based on the interviewer's assessment.

During the course of the site visits, it became clear that the P&S Plan had never really been implemented; however, some limited aspects had been initiated (notably, enhancements to data processing physical security and performance of background checks for terminal users and others having access to AJIS). Thus, the task of auditing conformance to the P&S Plan as originally designed did not seem feasible. Accordingly, a methodological change in the audit reporting approach was made. Rather than providing subjective ratings for the various elements of AJIS, we would simply identify a set of deficiencies and make recommendations for correcting

them. In accordance with the final audit methodology, findings and recommendations are presented in the following sections of this report. One key finding and recommendation will be highlighted.

It should be noted that deficiencies are not identified by site in this report--a separate, informal list of such site-by-site deficiencies has been submitted to the CJPA staff for consideration and possible corrective action.

III MAJOR FINDING AND RECOMMENDATION

During the course of the site visits, one major finding seemed to outweigh all others. This section will provide a discussion of that major finding, and the following section will present details of the specific deficiencies that were identified.

Major Finding

The major problem with the AJIS P&S program is that no well-defined P&S management program exists. There is no program being managed by a designated individual who has the responsibility for enforcement of regulations, the authority to alleviate P&S problems, and the responsibility to provide training and guidance to system users. There is no definitive set of standards, procedures, or guidelines describing the State statutes and regulations and how they apply to specific AJIS environments.

The P&S Plan of December 1975 was a step that should have been a start toward establishment of an AJIS privacy and security program; however, many elements of the plan were never implemented. Furthermore, although there is a designated AJIS Security Officer, his AJIS duties conflict with his other full-time duties (as a Public Safety Officer and as the State of Alaska NCIC and NLETS Officer). In addition, the AJIS Security Officer has no clerical assistance.

The lack of an AJIS P&S management program has led to a situation in which the P&S performance of the sites is a direct function of the awareness, knowledge, and management of the site supervisors, TSOs, and TOs. Despite the fact that their duties and responsibilities in AJIS P&S are ill-defined, the TSOs visited were aware of the importance of P&S measures, were all attempting to perform their function as best they could, and except for several instances, were judged to have developed and maintained an above-average level of security.

Another finding should be mentioned: there was a noticeable difference observed in both AJIS performance and the general level of P&S between sites in Anchorage and those in Juneau and Ketchikan. In Anchorage, there is far greater system activity, the response time for system transactions seems to be more rapid, the system is reasonably reliable, and the level of system P&S is quite good. In Juneau and Ketchikan, there is a lower level of system usage, the response time and system reliability are poor (response times on the order of 5 to 10 minutes during normal working hours are not uncommon, and system downtime reportedly is high--one Ketchikan site indicated it is not uncommon to be down all weekend), and the general quality of the P&S performance is not nearly as good as in Anchorage. Further, there is far less commitment or reliance on AJIS in the southeast. Without any formal analysis of this situation, it appears that the low system usage, the slow response time and poor system reliability, the distance from Anchorage, and the resultant inaccessibility of the ASO and AD correlate with a lack of commitment to AJIS. The conclusion that all of these factors affect the quality of P&S may well be generalized to other sites outside of Anchorage.

Primary Recommendation

Given the situation as described above, we make one primary recommendation which has a number of qualifying subrecommendations.

An AJIS P&S management program should be established. This program should be based on the P&S Plan of December 1975 and adhere to the applicable State statutes and regulations. The program should include at least the following elements:

- Development of a definitive set of AJIS P&S policies and procedures that describe P&S standards, procedures, and required documentation. It should be applicable to everyone coming in contact with AJIS, including system developers, users, TSOs, vendors, and visitors. It should be applicable to different types of facilities and equipment within the AJIS system. It is imperative that all those with access to AJIS must agree to conform to this set of policies and procedures.

- Establishment of a mechanism by which users (and possibly public members) are included in an AJIS committee that meets to

aid in the identification and resolution of P&S problems. This committee must have the power, within the constraints of the State statutes and regulations, to modify the AJIS P&S policies and procedures when warranted. Initially, the AJIS Committee that was recently appointed by Mr. Avrum Gross of the GCAJ could perform this function. As the P&S management program becomes firmly established, it may be more reasonable to establish a special AJIS P&S subcommittee that would take over most of the P&S functions. Final decision-making would remain with the GCAJ.

- Full-time dedication of the AJIS Security Officer to AJIS security and training duties; renaming this staff position as the AJIS Security and Training Officer (ASTO) may be desirable. This initiative must be accompanied by a commitment of sufficient resources for the accomplishment of the duties for the new position (including clerical assistance and materials) and funds for travel, document production, communications, educational activities, and so forth. A second person should be designated as an alternate in case the ASTO is unavailable.
- Assignment to the ASTO of responsibility for day-to-day enforcement and for training and guidance for system users, along with provision of sufficient authority to alleviate problems encountered.
- Assignment of responsibility to the AJIS P&S committee, along with the ASTO, for addressing and resolving the recommendations and deficiencies described in the following section as well as those determined in future audits.

The reasons for the high priority attached to the above recommendation are varied but important. Without an effective P&S management program, AJIS P&S will continue to flounder and be only as good as the individual sites make it in their more or less ad hoc approach. Furthermore, if there is such an operational program, it can be the focal point for rectifying the deficiencies discussed in the following section and identifying and solving other problems. There are a number of difficult tasks ahead if the recommendations in the following section are to be properly addressed and resolved. Furthermore, they must be resolved by those most familiar with the AJIS environment.

Another consideration is the benefits that will accrue to future audits. If a program is established that includes specific policies and procedures, future audits can be made more objective--that is, auditing conformance to an existing P&S program will not be nearly as subjective

as the current audit has been without the benefit of such a baseline effort.

As a potential aid to implementing some aspects of the major recommendation, it is suggested that SEARCH Group, Inc. (SGI) could be contacted. As described in a recent copy of their newsletter, Interface,* SGI is leading a new program funded by a grant provided through the LEAA (Law Enforcement Assistance Administration). This program offers on-site technical assistance in the area of P&S policy matters.

*SEARCH Group, Inc., Interface, Volume 4, Number 2 (June 1978), pages 6 and 13.

IV DEFICIENCIES AND RECOMMENDATIONS

The deficiencies noted in this section were identified during the audit process. Although not all of the deficiencies are considered major by themselves, as a group they are deemed significant. It is believed that had there been a P&S management program, as recommended in this report, most of the deficiencies noted would not exist. (The few deficiencies that do not fit this profile are not considered critical and therefore are not highlighted as described below.)

All the deficiencies need to be addressed in some manner, and the best way is through the implementation of the primary recommendation as previously described. The AJIS Committee should examine the deficiencies and determine the best solutions for rectifying them; requests for specific action should then be submitted to the GCAJ.

The remainder of this section is devoted to a table (Table 1) showing the deficiencies and associated recommendations. The table is organized such that related deficiencies are generally grouped together. Those deficiencies deemed to be of a more critical nature are highlighted by the placement of an asterisk before the description.

Table 1

ALASKA JUSTICE INFORMATION SYSTEM (AJIS)

RECOMMENDATIONS FOR IMPROVEMENT

	Deficiency	Recommendation
1.	The audit was unable to determine if the standards for conducting a background investigation have been prescribed by the GCAJ. [See CJIS P&S Regulations 6 AAC 60.040(a).]	If the standards have not been prescribed they should be so immediately and included in the AJIS Policy and Procedure Manual recommended in the primary recommendation of this report.
2.	No guidelines or standards have been established as to what constitutes sufficient reason to deny a person clearance.	Such guidelines should be prescribed along with the background investigation standards and included in the AJIS Policy and Procedure Manual.
*3.	Individuals occasionally use AJIS without proper clearance due to inability to go through current procedures on a timely basis.	There should be official recognition that the background investigation takes a considerable period of time (up to 6 months) by the establishment of a procedure for interim clearance. Guidelines should be established and included in the AJIS Policy and Procedure Manual. Further, the procedure for interim clearance should be timely, and no one should have access to AJIS terminals without at least an interim clearance.
4.	Terminal security agreements are not in general usage, and, where used, are not always current.	Terminal security agreements should be developed, and they should be signed by every TO before access to a terminal is granted or a password provided (this task was in the process of implementation in mid-June 1978). [See pages 74-77 in P&S Plan.]
5.	Procedures to follow when AJIS TOs and DP personnel terminate are not formalized, although TSOs generally do an adequate job.	Procedures that define the steps to take when AJIS TOs and DP personnel terminate should be formally established and placed in the AJIS Policy and Procedure Manual.
6.	The list of TSOs that was provided during the site visits (dated 2/10/78) had misspelled names, incorrect TSOs, incorrect agency names, and incorrect addresses.	The list of TSOs, their names, agencies, addresses, and telephone numbers should be systematically updated and maintained as currently and accurately as possible.

Table 1 (Continued)

Deficiency	Recommendation
7. The ASO seldom visits AJIS sites to provide P&S guidance—many sites and TSOs have never been visited by the ASO.	This can be addressed in the course of implementing the primary recommendation—make the ASO position full-time and provide sufficient funds for visits and training.
8. There is no agreement, formal or otherwise, with vendor or custodial personnel (especially RCA) for sanctions or other actions that can be taken against them if the P&S regulations are not adhered to.	Include vendor and custodial personnel in the AJIS P&S management program, including the signing of agreements, issuance of clearances, definition of access (if any), as well as identification procedures required at the user and DP sites.
9. The AJIS-supplied header on outputs is too cryptic to be of broad use in the aid of document control.	Provide a less cryptic header for all AJIS outputs that can be well understood by those not familiar with the system.
10. AJIS outputs are often produced using only several lines of print and only minimal spacing is provided between outputs. Users often deal with small slips of paper that are easily misplaced or lost and that are difficult to file. Also, there is often too little room for a confidentiality stamp (see next item).	Provide a standard or minimum size for all AJIS output so as to aid in avoiding this problem.
11. Few agencies are stamping (or even have a stamp for) their AJIS output to indicate its origin and confidentiality.	Either a system-wide confidentiality stamp should be developed and mandated for use by all terminal sites or the outputs should all be marked automatically as a normal part of the output process. [See page 77 in the P&S Plan.]
12. Dissemination logs are not standardized and are not used by all terminal sites (the major noted non-use was by law enforcement agencies that were providing driver information to be attached to all driving citations that are given to district attorneys—a practice that can result in hundreds of transactions per day).	A standardized dissemination log should be developed and mandated for use by all terminal sites. Exceptions may be granted where appropriate (e.g., when one agency is providing information for use by another authorized state agency on a regular basis and the receiving agency does not yet have a terminal—automated logs should be developed to provide for this situation until all authorized agencies obtain their own terminals).
13. Computerized dissemination logs are not maintained.	A process for the development and implementation of computerized logs should be addressed. [See P&S Plan, pages 60-61.]

Table 1 (Continued)

Deficiency	Recommendation
14. A list of agencies authorized to receive AJIS information as well as the agreement forms they have signed is maintained by AST Records and Identification in Juneau. A list of agencies not authorized to receive AJIS information has been provided to users, yet few, if any, users are aware of specifically which agencies can or cannot receive such information.	A list of agencies that are authorized to receive AJIS information (as well as those not authorized) should be made available to all TSOs and a method devised to continually make TSOs aware of the list.
*15. Document destruction procedures are not defined for the user sites and the DP facility, and at a number of sites current practices are not such that proper destruction of AJIS originals, second copies, or carbon paper (where it is used) is ensured.	Define and enforce document destruction practices for all terminal sites and the data processing facility. If second copies are not needed, eliminate two-copy paper for the terminal printers at such sites. Use of destruction capabilities possessed by other local agencies should be considered.
*16. Passwords assigned to the TOs are changed approximately every 2 months—a TO is assigned a different password for each accessible terminal; thus, some TOs can have four or more active passwords. The passwords are not chosen by the TOs but are predetermined, and they are mailed along with those for all TOs at a site to the site TSO. Some problems were found with the current process, although the use of passwords is a key security feature of AJIS: • The list of TSOs that was obtained during the site visits was not up-to-date in at least one instance. In such a case it is unclear who the recipient of the passwords would be at the user site. • The address of one terminal site was incorrect, and passwords have been going to the wrong agency. Requests for change of address did not lead to a correction. • Passwords are mailed in the regular mail, and at some sites this mail is opened by persons other than the addressee.	Several steps should be considered for modifying the process of assigning passwords: • Maintain an up-to-date and accurate list of TSOs and their addresses. (See also Item 6 in this table.) • Mail passwords to the TSOs by either certified or registered mail in an envelope that clearly indicates it is to be opened only by the addressee (or a designated alternate in the event the TSO is unavailable). A double envelope process could be implemented, with the inside envelope containing the instructions for opening. • If possible, the system should be modified to provide only one password per TO. That password could be acceptable for use on a specified set of terminals.

Table 1 (Continued)

Deficiency	Recommendation
• TOs with more than one password are usually forced to keep the various passwords on paper somewhere so that they can refer to them when necessary, thus creating a situation where it is easier for non-cleared persons to obtain the passwords.	
17. The log-on process is such that passwords are typed and are potentially visible to other persons in the terminal area.	If possible, the log-on process should be modified so that passwords are not decipherable to persons in the terminal area, either by not displaying any of the password characters or by overwriting the password characters by other characters so that the password is unreadable.
*18. A number of sites visited did not have a lockable terminal room to better provide for physical security during non-operational hours. All had lockable offices or were controlled environments, such as law enforcement and correction agencies, that were operational 24 hours per day.	Where appropriate, terminal sites should have a separate, lockable terminal room, or a method for physically locking the terminals to provide for security during non-operational hours.
*19. Some AJIS terminals are located in areas where there is a good deal of activity, either from non-cleared office personnel or from visitors who have legitimate business. Terminals were also observed located with office files, and one terminal was located with the office copy machine.	Insofar as is possible, terminals should be located in areas that are not used for normal office activities such as visitor reception, storage of office files, or document copying activities.
20. Terminals at some sites with desk areas that serve the public are faced so that visitors can see the display screen. Not all were readable (either they were slightly too far away or not in a direct line of sight), but one was completely visible and readable.	Define and mandate specifications for the placement and physical orientation of AJIS terminals, especially at sites that normally serve the public.
21. Administrative messages are sent and received by personnel other than cleared TOs at AJIS terminals, thus giving them access to the terminal and terminal area. Although such usage does not require a password, usage does occur on terminals	Non-cleared personnel should not be given access to terminals for other than AJIS activities while the terminal is logged on with a valid password. Security standards should be developed and included in the AJIS Policy and Procedure Manual (see primary recommendation)

Table 1 (Continued)

Deficiency	Recommendation
that have not been logged off—i.e., the terminal is still in "AJIS mode."	that specify access, if any, to be granted to non-cleared personnel for use of AJIS terminals for administrative messages. (See also Item 3 in this table.)
22. Many user sites have emergency power capability, but in general, terminals tend to not be connected to the emergency circuits. Thus, a power failure at a site renders the AJIS terminal inoperative.	Where emergency power systems exist, steps should be taken to ensure that the AJIS terminals are connected to the emergency circuits.
23. Few sites have reasonable manual backup capabilities in the event of catastrophic system failure.	The problem of providing for reasonable manual backup capabilities at the various AJIS sites should be addressed as a systemwide concern. The current system backup capabilities must be addressed first, and manual backup should become an integral part of the design considerations for each new module.
24. Formalized training in AJIS capabilities is almost non-existent, and training documents are inadequate and out-of-date. Privacy and security are not sufficiently integrated into existing training or training documents, either systemwide or at the local level. Further: • The ASO does not conduct security orientation sessions at each terminal location (or at any terminal location). • There is little or no training provided by the ASO for each new operator or data center employee on AJIS operation, terminal operation, or P&S controls. • There is no training manual that permits all AJIS locations to train their own personnel should the TO not be available to perform this task (some limited training aids have been developed and used at some user sites). • There is no AJIS Training Officer.	Training programs and procedures should be formalized and implemented, including the establishment of the training officer position or function (see the primary recommendation for the ASTO position). [The basis for this program should be that specified in the P&S Plan, page 77.]

Table 1 (Continued)

Deficiency	Recommendation
25. Training sometimes occurs by one agency training personnel from another agency. Thus, TOs can be trained for the use of transactions that are not available at their own site.	Training should occur for TOs only at their own sites (or those so designated by the ASO), using their assigned password.
26. Training occurs using real data, a practice that is a violation of the "spirit" of the rights of personal privacy.	(See following recommendation.)
27. There is no test mode or associated test files for use in system development, maintenance activities, demonstrations, or training activities.	A test mode and an associated set of test files should be developed and implemented for the following uses: • Development, testing, and debugging of AJIS software by DP personnel. • Maintenance activities by vendor personnel. • Demonstrations of system capabilities to visitors and other non-cleared personnel. • Training of terminal operators.
28. The AJIS backup files are maintained up-to-date both on- and off-site, but they are not well protected from destruction by fire, as required by State regulations.	As per State Regulation 6 AAC 60.030(d), when not physically on the computer, recorded AJIS information is to be kept in a fire-resistant, locked facility at or near the computer facility. At least one copy of the backup files (and preferably both) should be so stored.
29. Although the DP facility has excellent physical security and all persons with access to the terminal are cleared, there are no formal controls or procedures that specify the DP personnel's access to the AJIS software and data files.	There should be a provision for the specification of formalized procedures (including possible use of audit trails) for the controlling and monitoring of access to AJIS software and data files by DP personnel. Such procedures should not adversely affect performance.
30. The former AJIS Director did not develop a disaster plan, as called for in the P&S Plan, that covers individual responsibilities and actions to be taken should a disaster be imminent, including: alternate processing facilities; rebuilding the communication network; restoration of files; fire alarm procedures; fire control and detection; fire, police, and guard liaison procedures. The plan should also address other natural and man-made disasters.	The plan should be developed. [See pages 78-80 in the P&S Plan.]

Table 1 (Continued)

	Deficiency	Recommendation
*31.	There is no possibility of computer back-up in the event the AJIS computer becomes inoperable for an extended period of time.	Future plans and design for AJIS hardware modification or upgrade should include considerations for providing alternate (or redundant) processing capabilities and/or components in the event of catastrophic system failure. It would also be advisable for future State DP procurements to consider the provision of backup capability for the AJIS computer facility.
*32.	There is no uninterruptable power source (UPS) for the AJIS computer facility.	Provision should be made for UPS for the AJIS computer facility and its major components, including teleprocessors and terminals, where deemed appropriate. Such capability should be tested on a regular basis.
*33.	There is no document (as described on page 83 in the P&S Plan) that is available to individuals from any criminal justice agency that describes the rules of access by individuals, including: where reviews are conducted; hours of review; fees charged; procedures for verification of identity; form for making challenges; and rules for submitting explanatory material.	The rules of access for individuals should be developed and made available to individuals at any criminal justice agency.
34.	Outside of the log of individuals who request access to AJIS information for themselves (and a consistent form is not used in all agencies), forms for challenges, administrative review, and administrative appeal have not been formalized and procedures have not been defined or mandated for use at terminal sites for individual right of access.	Individual right of access procedures need to be formalized and placed in the AJIS Policy and Procedure Manual to be developed as a part of the primary recommendation, using as a basis the State statutes and regulations as well as the P&S Plan. [See pages 84-90 in the P&S Plan.]
35.	The manner in which State regulations define agency access to various information in AJIS will require that in order to obtain all the information contained in AJIS on himself, an individual will need to visit at least two agencies. Individuals will probably view this procedure as a "run around."	This problem needs to be addressed and resolved by the AJIS Committee. Some advocates of the rights of individual privacy view separation as a necessary safeguard. However, if a "run around" is to be avoided, State regulations could be modified so that selected sites and individuals at those sites would be designated to handle all requests and be given the authority and capability to provide the requisite information.

Table 1 (Continued)

	Deficiency	Recommendation
*36.	One site was found to be providing driver information in response to written requests from insurance companies.	The site TSO was told that this practice should be discontinued immediately, and CJPA was notified of the specifics of this deficiency. As driver information is constantly being sought by insurance companies, it is suggested that all TSOs be immediately notified of the applicable State statutes and regulations.
37.	Not all AJIS agencies have a terminal, and as a result they occasionally rely on other AJIS agencies with terminals to provide them with AJIS information.	Either agencies that require AJIS information as a normal activity should acquire AJIS terminals, or some method of sharing terminals should be considered where appropriate. (See also Item 12 of this table.)
38.	The poor system response time creates potential security problems. If an operator must wait 5 to 10 minutes to complete one transaction, it is likely that the terminal will be left unattended during the waiting period.	System response time must be improved considerably.
39.	The courts computer system does not come under the State P&S statutes and regulations for criminal justice information systems. This creates a dual standard—there is information in both AJIS and the courts system that is essentially the same, yet the information must be handled differently.	The dual standard for P&S of information in AJIS and the courts system should be examined by the GCAJ and potential solutions posed, including the possible development of regulations for criminal justice information systems that do not fall under the current State statutes and regulations.
40.	Users are generally unaware of which vendor (primarily RCA) maintenance personnel are cleared.	A method of identifying vendor and custodial personnel who are cleared for access to the terminal areas should be established and included in the AJIS Policy and Procedure Manual (See also Item 8 in this table.)
*41.	At least two RCA facilities maintain "free wheeling" monitor terminals to provide more effective aids in determining system problems as they occur. RCA is not an authorized criminal justice agency or subunit, yet it has access to all AJIS information (but only as viewed when monitoring the activity of user terminal circuits).	The question of RCA access to AJIS information is one that needs immediate resolution (by the AJIS Committee and the GCAJ)—a resolution that will not significantly reduce current capability to respond to maintenance requests. Possible considerations include: • Designation of RCA as a criminal justice agency subunit by the Governor. • Designation of individuals at each RCA site as TSOs.

Table 1 (Concluded)

Deficiency	Recommendation
	• Execution of a user agency agreement with RCA. • Execution of TO agreement forms with each RCA employee who has potential access. • Clearances (through background investigations) for all RCA individuals with potential access. • Maintenance by RCA of a log for service calls, use of the monitor, and AJIS site visits as a method for monitoring access. • Creation of definitions and standards for RCA terminal site security procedures. • Provision for test file usage when RCA must monitor a line. • Provision for the physical security of the terminals, including either a locked room or cabinet, or a physical terminal lock and control of keys. • Provision of up-to-date ID cards for cleared RCA personnel at all user sites. • Site visits and spot checks by the ASO. • Designation of local coordinators (non-RCA) who receive all service requests, check out potential solutions, and call to authorize RCA monitor troubleshooting only when needed.

*Deficiency deemed to be more critical than others.

Appendix A

SITE VISIT SCHEDULE

ANCHORAGE

12 June 1978

SITE	TIME	PERSON(S) INTERVIEWED
Alaska State Troopers	0800 hours	Sgt. Robert K. Crank, AJIS Security Officer
Div. of Data Processing	1100 hours	Dale Griggs, AJIS Director and Assist. Director of Data Processing
Anchorage Police Department	1445 hours	Adriana Tolson, Terminal Operator
		Capt. Weaver

13 June 1978

City Attorney's Office	0830 hours	Shirley Otte, Terminal Security Officer
Alaska Courts	1010 hours	Linda Pinkston, Information Systems Supervisor and Terminal Security Officer
State Attorney's Office	1350 hours	Mary Purvis, Terminal Operator
Probation & Parole	1500 hours	Judy Lavar, Terminal Security Officer

JUNEAU

14 June 1978

SITE	TIME	PERSON(S) INTERVIEWED
Alaska Courts	0830 hours	Dolores Beierly, Terminal Security Officer
Alaska State Troopers, Records & Identification	1000 hours	Bill Brown, Supervisor of Records and Identification and Terminal Security Officer
RCA	1330 hours	Claude Purvis, Supervisor
Corrections	1500 hours	Bill Peterson, Terminal Security Officer

15 June 1978

Juneau Police Department	0830 hours	Sgt. Dennis Windred, Terminal Security Officer
Probation & Parole	1000 hours	Kermit Humphries, Terminal Security Officer Kari Rapplanger, Terminal Operator
Alaska State Troopers, B Detachment	1330 hours	Capt. John P. Monagle, Terminal Security Officer
Motor Vehicles	1500 hours	Lee Standiford, Terminal Security Officer

KETCHIKAN

16 June 1978

SITE	TIME	PERSON(S) INTERVIEWED
Alaska State Troopers	0830 hours	Sgt. Morris T. Rodgers, Terminal Security Officer
Corrections, Detention Home	1030 hours	Richard Pearson, Terminal Security Officer
		Robert Andrew, Terminal Operator
Motor Vehicles	1330 hours	Unannounced -- did not talk with anyone.
Ketchikan Police Department	1400 hours	Chief R. F. Hackstack

Note: Attempted to visit Fairbanks Police Department on 10 June, but Terminal Security Officer away for weekend.

Appendix B

AUDIT OF AJIS PRIVACY AND SECURITY PERFORMANCE
INTERVIEW FORM

Interviewer: _____ Date: _____

Interviewee: _____ Time: _____

Title: _____ Place: _____

Agency: _____

_____

AJIS Involvement: _____

_____

_____

_____

_____

Length of AJIS Involvement: _____

_____

Audit Area	Rating
Personnel Selection	
Physical Security	
Individual Right of Access	

Subjective Rating Guide

Rating	Definition
5	Superior: No improvements necessary; exemplary; outstanding.
4	Above Average: Minor improvements would make the system superior in this area; commendable; well done.
3	Acceptable/Average: Significant improvements necessary; satisfactory performance; sufficient.
2	Deficient: Major improvements necessary; mediocre; insufficient.
1	Very Poor: Generally ineffective; unsatisfactory.
0	Unacceptable: Complete overhaul required.
N/A	Not applicable.

STATE OF ALASKA

CRIMINAL JUSTICE INFORMATION SYSTEM
TERMINAL SECURITY CLEARANCE AGREEMENT

I,_____, have read and am aware of my security
(Print Name)
responsibilities as related to criminal justice information, as well as the fines and punishment provided for under AS 12.62.060, AS 12.62.070, 6 ACC 60.040(a) and (c). I have also read and am aware of the requirements governing release to unauthorized persons pursuant to Title 28, Chapter 1, Part 20.

I understand that:

1. All inquiries made or requested by me to any Criminal Justice Information System data bank will be job related.

2. I will not obtain for, or show to any person, their own Criminal Justice Information System record without a signed approval from my Terminal Security Officer.

3. I understand that no Criminal Justice System information obtained on a terminal will be given to any other agency without the signed approval of the Terminal Security Officer.

4. Should I be assigned a "Password", I will not allow anyone access to my AJIS "Password" other than the Terminal Security Officer, Divisional Security Officer, or Alaska State Trooper Security Officer. Further, I will read and abide by the provisions set forth in the AJIS Users Guide, pages 7-1 through 6-15, inclusive.

5. I understand that violation of any condition set forth is sufficient grounds for disciplinary action to be initiated against me as per policy and procedures.

Please check the appropriate box below:

[ ] I wish to have a Criminal Justice Information System Security Clearance, and agree to the terms and conditions set forth in this agreement.

_____ _____
Signed Date

[ ] I do not wish to have a Criminal Justice Information System Security Clearance.

_____ _____
Signed Date

[ ] Affirmative Security Agreement Date_____ Checked By_____

[ ] Fingerprinted Date_____ Checked By_____

[ ] Background Investigation Date_____ Checked By_____

[ ] AJIS Security Regulations (if password to be assigned) Date_____ Checked By_____

[ ] Terminal Check Out (if password to be assigned) Date_____ Checked By_____

Personnel Selection

The CJIS Regulations provide: AAC 60.040. TERMINAL SECURITY.

(a) A background investigation by a law enforcement agency adhering to standards prescribed by the commission shall be conducted with respect to all personnel who have access to a criminal justice information system terminal in an operational environment prior to being assigned to that terminal.

Are the current elements of the CJIS Statute and Regulations regarding Personnel Selection being adhered to, and are they adequate?

- Have all personnel who have access to an AJIS terminal had a background investigation conducted by the AJIS Security Officer prior to assignment?

  How many individuals have such access?

  Are any non-cleared personnel ever allowed access to the terminal or terminal environment (e.g., custodians, maintenance or other vendor personnel, etc.)?

  Is there any provision for conducting periodic background or record checks on cleared individuals?

  Are there any provisions for termination procedures for individuals with terminal access, and, if so, are they being followed?

  Are there periodic and/or spot-check audits of any of the hiring, monitoring, and termination procedures?

- Have terminal security clearance agreements been executed for each potential terminal operator prior to terminal access?

  Are they complete, up-to-date, and on file?

  Are the training programs and procedures currently formalized, are they being conducted, and are they adequate?

  Is there formal training provided for each new operator or data center employee on AJIS operation, terminal operation, and security and privacy controls, and is such training provided on a continuing basis?

  Does the AJIS Security Officer visit each terminal location to conduct security orientation sessions with terminal security officers, terminal operators, criminal justice users, and non-criminal justice users?

  Has a training manual been developed that permits training by local personnel at each terminal location in the event the AJIS Training Officer is not available to perform this task?

Do the training and orientation sessions provide for discussion on the needs and methods for the control and destruction of hard copy output?

- Are all active copies of AJIS-produced criminal justice information properly stamped, controlled, and accounted for?

- Does each terminal location have a designated terminal security officer who has the day-to-day responsibility for the conduct of the security and privacy program and procedures?

  Are the terminal security officer's duties and responsibilities well defined?

  Is the terminal security officer doing an effective job?

Physical Security

The CJIS Security and Privacy Regulations provide: 6AAC 60.040.

(b) Physical plant security shall be provided by all agencies with access to a computerized criminal justice information system to insure maximum safeguards against fire, theft and all unauthorized entry to areas where criminal justice information is stored, processed or disseminated.

Is the physical plant security required to be provided by agencies with access to AJIS computerized criminal justice information adequate to insure maximum safeguards against fire, theft, and all unauthorized entry to areas where criminal justice information is stored, processed, or disseminated?

- Are there comprehensive facilities plans and practices (e.g., the AJIS Director developed disaster plan) that consider adequate utility supplies and exterior protection from both natural and man-made forces?

  Are there procedures in effect that consider protection of the exterior of the facilities with respect to both natural (fire, water, storm, earthquake) and man-made forces (strikes, riots, sabotage, accident, bomb threats, mischief)?

  Are there procedures in effect that consider the provision of adequate utilities and supplies for system backup in the event of unforeseen stoppages?

  Are the protection procedures and the backup capabilities adequate?

  Have the protection procedures and the backup capabilities and procedures been tested, and if so, were they adequate?

  Are the procedures and capabilities adequate for the protection and backup of the system now?

  Does the AJIS disaster plan adequately address the following areas:
  - Alternate processing facilities
  - Rebuilding the communication network
  - Restoration of files
  - Fire alarm procedures
  - Fire control and detection
  - Fire, police, and guard liaison procedures

- Are the interiors of the building complexes designed and used to aid in control of personnel access to sensitive areas?

  Are the interiors of the building facilities designed to aid in the control of sensitive areas of criminal justice operations?

Are the facilities used to aid in the control?

Is the design and the use of the facilities with respect to the control of personnel access to sensitive areas adequate?

Are there procedures or controls in effect concerning the limiting of physical access of all persons to buildings, computer rooms, data storage rooms, terminal rooms, terminals, and so forth?

Is there a means of identification for all personnel in the form of badges, cards/keys, identification cards, guards, receptionists, etc. in all of the above areas?

Are the procedures and controls questioned above being followed?

Are there procedures in effect to audit the physical access practices, e.g., examination of logs of persons in sensitive areas, checking of practices with respect to changes in personnel status, spot checking, and so forth?

Are there security procedures in effect that pertain to: password and identification mechanisms (initiation, changes, deviation, audit), fire and safety drills, backup and recovery exercises (catastrophic plan), intra-agency activities (data exchange, system usage, conflict resolution--also the same activities in an inter-agency basis and with the public), risk analysis, security/audit analysis, formulation and adherence to a code of ethics, special data handling for sensitive data and programs, inventory control, data entry and modification control of systems output (logs, labels, etc.), purge criteria, and so forth?

Are the terminal rooms and/or the terminals capable of being physically locked?

Are the security procedures or practices questioned above being followed?

Software may be generally categorized as those programs normally associated with the operating system, those that provide the tools with which programmers interface to the system (language processors and utility programs), those that typically take the form of packages or predeveloped subsystems, and application programs.

- Is the development of software and the modification and maintenance of implemented software performed in a secure fashion so as to help ensure the integrity of information systems?

  Are controls for software and for information system generated data stored off-line adequate to ensure proper security, backup, and information system recovery?

  Is on-line access to information system software and data adequately defined and controlled?

  Are there procedures or practices in effect to aid in the safeguarding of security and privacy of information with respect to programs in the following areas: design activities, development activities, test activities, implementation activities, maintenance activities (up-date and extension), backup capabilities, access (system developers, users, others), user identification, audit activities (access, modification, etc.), handling of system documentation, and so forth?

  Are the above procedures being followed, and, if so, are they effective?

Data may be generally categorized as on-line or off-line, but may be available in varying forms, on varying media, and at different locations; e.g., disk, tape, core, listings, CRT screens, forms, cards, on-site, library, and so forth.

- Are there procedures or practices in effect to aid in the safeguarding of security and privacy of information with respect to data stored off-line (and off-site), including identification of authorized personnel, control of documents and other data media, adequacy and accuracy of backup data, and so forth, and, if so, are the procedures being followed, and are they effective?

Are there procedures or practices in effect to aid in the safeguard of security and privacy of information with respect to on-line access to software and data, including identification of authorized terminals, identification of authorized personnel, controls to restrict access to a subset of programs and/or data controls to restrict certain activities to identified users and/or terminals (e.g., update, purge, etc.), audit activities, and so forth?

Are procedures being followed, and are they effective?

Are the controls adequate, and are they effective?

Does the control of disseminated data extend beyond the receiving agency?

Individual Right of Access

The Alaska CJIS Security and Privacy Statute and Regulations specify in detail the individuals right of access. The Statute provides (Sec. 12.62.030):

> (c) A person shall have the right to inspect criminal justice information which refers to him. If a person believes the information to be inaccurate, incomplete or misleading, he may request the criminal justice agency having custody or control of the records to purge, modify or supplement them. If the agency declines to do so, or if the person believes the agency's decision to be otherwise unsatisfactory, the person may in writing request review by the commission within 60 days of the decision of the agency. The commission, its representative or agent shall, in a case in which it finds a basis for complaint, conduct a hearing at which the person may appear with counsel, present evidence, and examine and cross-examine witnesses. Written findings and conclusions shall be issued. If the record in question is found to be inaccurate, incomplete or misleading, the commission shall order it to be appropriately purged, modified or supplemented by an explanatory notation. An agency or person in the state with custody, possession or control of the record shall promptly have every copy of the record altered in accordance with the commission's order. Notification of a deletion, amendment and supplementary notation shall be promptly disseminated by the commission to persons or agencies to which records in question have been communicated, as well as to the person whose records have been altered.
>
> (e) Reasonable hours and places of inspection, and any additional restrictions, including fingerprinting, that are reasonably necessary both to assure the record's security and to verify the identities of those who seek to inspect them may be prescribed by published rules. Fingerprints taken under this subsection may not be transferred to another agency or used for any other purpose.
>
> (f) A person or agency aggrieved by an order or decision of the commission under (c) of this section may appeal the order or decision to the superior court. The court shall in each case conduct a de novo hearing and may order the relief it determines to be necessary. If a person about whom information is maintained by any agency challenges that information in an action under this subsection as being inaccurate, incomplete or misleading, the burden is on the agency to prove that the information is not inaccurate, incomplete or misleading. (§ 1 ch 161 SLA 1972).

The Regulations state:

6 AAC 60.080. INDIVIDUAL'S RIGHT TO INFORMATION. Each individual shall have the right to review criminal justice information relating to him. Each criminal justice agency in this state with custody or control of criminal justice information shall make available facilities and personnel necessary to permit review of criminal justice information for which access has been authorized under sec. 60 of this chapter. Reviews shall be conducted in accordance with the following procedures:

(1) Reviews shall take place only within the facilities of an agency authorized to have access to criminal justice information under sec. 60 of this chapter, and only under the supervision and in the presence of a designated employee or agent of a criminal justice agency.

(2) Reviews shall be permitted only after proper verification that the requesting individual is the subject of the criminal justice information he is seeking.

(3) A record of each review shall be maintained by criminal justice agencies. Each review form shall be completed and signed by the supervisory employee or agent present at the review. The form shall include a recording of the name of the reviewing individual, the date of the review, and whether or not any exception was taken to the accuracy, completeness or contents of the information reviewed.

(4) An individual exercising his right to review criminal justice information may compile a written summary or make notes of information reviewed, and may take with him copies thereof. Individuals may not, however, take any copy that might reasonably be confused with the original.

(5) Each individual exercising his right to review criminal justice information shall be informed of his right to challenge the inclusion of information, pursuant to AS 12.62.030(c) and (f) (Eff. 10/09/72, Reg. 44; am / /73, Reg. 45).

Are the procedures regarding an individual's right to information from AJIS being properly administered and is the administration adequate and in conformance with existing statutes and regulations?

- Do reviews take place only within the facilities of agencies authorized to have access to criminal justice information and only under supervision and in the presence of a designated employee or agent of a criminal justice agency?

  Are reviews conducted only after proper identification that the requesting individual is the subject of the criminal justice information being sought? Is the verification by fingerprint comparisons in the case of a criminal record review and by two forms of identification if a non-criminal record review?

  Is the record of each review maintained by criminal justice agencies, including the name of the reviewing individual, the date of the review, and whether or not any exception was taken to the accuracy, completeness, or contents of the information reviewed?

- Are reviewing individuals allowed to compile a written summary or make notes of information reviewed and able to take these upon departure? Are reviewing individuals denied the right to take any copy of reviewed information that might reasonably be confused with the original?

- Is each individual exercising his right to review criminal justice information informed of his right to challenge the inclusion of information pursuant to AS 12.62.030(c) and (f)?

- Is there a document that is available to be given to individuals by any criminal justice agency upon request that covers:
  - where reviews are conducted
  - hours of review
  - fees charged
  - procedures for verification of identity
  - form for making challenges
  - rule for submitting explanatory material?

- In the event that a record is found to be inaccurate, incomplete, or misleading and the Commission orders it to be purged, modified, or supplemented by an explanatory notation, are the rules for correction procedures being followed and are they adequate (i.e., is the record altered, a notification promptly disseminated to the persons and/or agencies to which the records in question have been communicated as well as to the person whose record has been altered, are logs being maintained of of these transactions, are the agencies that receive notice of correction modifying any and all reports or files that might contain the erroneous information)? Are there procedures to provide for error correction of records that have been further disseminated by a receiving agency to yet another authorized agency?
- Are the rules with respect to administrative review being followed and are they adequate once a record is challenged by a reviewing individual (i.e., review of challenge and submission within 15 working days of a notice of the results of the audit to the challenging individual)?
- Are the rules with respect to administrative appeal being followed and are they adequate if a challenging individual believes an agency's decision during administrative review to be unsatisfactory?
- Is a reviewing individual given access to <u>all</u> the information being maintained on him by AJIS at the time of the review?

ALASKA JUSTICE INFORMATION SYSTEM

AJIS Form No. 1

Date_____

REVIEW OF CRIMINAL OFFENDER RECORD INFORMATION

1. Name and location of agency:_____

_____

2. Name of supervisory employee:_____

3. Name of reviewing individual:_____

4. Records reviewed:_____

_____

Name of individual to whom records relate:_____

Identification number:_____

5. Did the reviewing individual express any challenge to the accuracy or completeness of the information reviewed?_____ If he did so, to what portions of the information? _____

_____

_____

6. Verification. Note: Completion of this item is voluntary.

I have reviewed the records described above and have found no errors or omissions therein.

_____

Signature of reviewing individual

Date of Verification: _____

7. Note: Each reviewing individual shall be informed of his rights of challenge under these regulations.

ALASKA JUSTICE INFORMATION SYSTEM

AJIS Form No. 2

EXCEPTIONS TAKEN TO CRIMINAL OFFENDER RECORD INFORMATION

1. Name of individual submitting exceptions: _____

_____

2. Name of agency: _____

3. Records to which exceptions taken: _____

_____

_____

Name of individual to whom records relate: _____

Identification number: _____

4. Summary of exceptions and reasons therefor: _____

_____

_____

_____

_____

_____

5. Verification.
I affirm that I have taken the above-described exceptions, that those exceptions are taken in good faith, and that they are to the best of my knowledge true.

_____
Signature of Individual

Date of Verification: _____

ALASKA JUSTICE INFORMATION SYSTEM

AJIS Form No. 3

Notice of Results of Audit of
Criminal Offender Record Information

To:_____

_____

_____

Pursuant to exceptions taken on_____,

19_____, by_____to criminal offender record

information within the custody or under the control of_____

_____an audit of the information has been conducted

and, in accordande with the results of that audit, the exceptions have been

_____. The following actions

have been taken, or now are in progress, to implement the audit's findings:

_____

_____

_____

_____

_____

(Name of criminal justice agency
conducting the audit.)

Dated:_____

END