



**Alaska Law Enforcement Sharing System
ALEISS
Privacy Impact Assessment**

September 3, 2004

Contact Points

Maxine Andrews, Program Manager
National Law Enforcement and Corrections Technology Center - Northwest
(907) 569-5685

Assistant Chief of Police Greg Browning, ALEISS Chairman
Juneau Police Department
(907) 586-0680

I. Introduction

The Alaska Law Enforcement Information Sharing System (ALEISS) Consortium, formed in September 2003 to accomplish the following goals:

1. Identify technology that will facilitate the sharing of law enforcement information across jurisdictional boundaries and across multiple disparate records management systems for the purpose of increasing the efficiency of criminal investigations
2. Identify funding sources to accomplish this goal

II. System Overview

COPLINK from Knowledge Computing Corp. of Tucson, Arizona, was the commercially available software solution chosen.

What is the nature of data?

The data shall include Law Enforcement business records ALEISS Consortium Member Agency maintained for the purpose of conducting criminal investigations and law enforcement activities. Information regarded as “criminal intelligence data” shall not be regarded as Law Enforcement Information and will not be included in the ALEISS data repository. The data will be composed only of data currently being collected by the respective agencies. No additional data will be created or included by ALEISS.

Why is information being collected?

To provide a solution to the problem of slow information exchange between law enforcement agencies due to disparate law enforcement information systems that lack a common language or a compatible database platform. Secondly, to provide sophisticated analytical tools to enable law enforcement investigators to discover links and relationships by providing consolidated data that may allow them to solve previously “unsolvable” incidents and prevent serial criminal activity.

What is the intended use of the data?

The data is intended to be used in conjunction with bona fide criminal investigations and other legitimate law enforcement activities. While the intent is to provide law enforcement officers with cross-jurisdictional information that is reliable, it is understood that the information should be verified by further investigation and/or contact with the source agency.

What are the sources of data? How is the data acquired?

The data will be exact copy of a subset of participating agency’s records management systems (RMS) data. Each participating agency determines what information they are willing to contribute to ALEISS. Data will be acquired by automated updates on a predetermined schedule (varies with agency, correlates to data volume.) Section 8.1 of the ALEISS Security Directive document addresses this issue in more detail.

How will data be checked for accuracy?

ALEISS will not conduct systematic data accuracy checks because this function is the responsibility of each contributing agency. Agencies whose data is found to be questionable will be notified and the agency is responsible for verifying and correcting their source data. The data in the ALEISS node is “read only” and must be changed at the source. Once the source data is corrected, the ALEISS node will reflect that correction at the next refresh cycle. ALEISS users are tasked with discrepancy notification responsibilities. Should they encounter discrepancies, users are asked to note the contributing agency, document number,

and any relevant details, then forward that information to the ALEISS System Administrator who notifies the contributing agency.

Will newly derived data become part of individual's record?

Newly derived data will become part of an individual's record and will be reflected on the ALEISS node at the next refresh cycle.

How will data be verified for relevance and accuracy?

Data on the ALEISS node is an exact replica of the data from the contributing agency's RMS. The burden of relevance and accuracy resides with each contributing agency. The data will be no more or less accurate than it would be without ALEISS.

Are data elements described in detail and documented? If so, what is the document to be referenced?

Data elements are described in the User Guides. A User Guide is available on the ALEISS web site.

What opportunities do individuals have to decline to provide information?

Individuals have no opportunity to decline to provide information. Individual's information is provided by participating agencies, based on their contact with or involvement in a law enforcement activity. If an individual has had no contact with at least one of the member police agencies, they normally would not be included in the ALEISS data.

What opportunities do individuals have to consent to use of information?

Individuals have no opportunity to consent to use of information. However, individuals who have not had police contact would normally not be included in the system.

How do individuals grant consent re: use or sharing of information?

Information maintained by ALEISS is a subset of that maintained by its member agencies, who gather it as a normal course of Law Enforcement activities and investigations. "Intelligence," or information not verified by investigation, is not a part of ALEISS. Police agencies are not required to obtain consent from individuals who are arrested or subject to police investigation to maintain records of such contacts and the results of the police activity. As this information is only shared with authorized individuals from other Law Enforcement Agencies, permission is not sought before sharing this information.

What are procedures for correcting erroneous information?

Data that is suspected to be erroneous will be referred back to the contributing agency. If an error is confirmed, the source data will be corrected at its source, and the ALEISS node will reflect that correction at the next refresh cycle.

Who will have access to data (users, managers, sysadmin, developers)? Is it documented?

Data access is limited to qualified law enforcement agency employees, system administrators, and developers. The ALEISS Security Directives Document section 5.1 Eligibility details the necessary qualifications for system access. Section 5.2.1.3 further details eligibility.

How will access be determined?

Access is governed by strict requirements; including a fingerprint based background check and legitimate need. Access is determined by individual member agencies subject to the ALEISS Security Directives. Qualified users will receive a login and password. System access is allowed only after an authorized login and password have been entered.

Are criteria, procedures, controls, responsibilities documented?

All system users are required to read and acknowledge the ALEISS Security Directives Document and receive training prior to receiving their login and password. These requirements are documented on the ALEISS User Application Form and witnessed by the agency ALEISS Officer.

Will users have role-based access?

Users will have a role-based access. There are three levels of data access determined by the ALEISS Security Directives and individual agency preference. These data access levels are detailed in The ALEISS Security Directive Document Section 7.1 "Read Only" Access Levels.

What controls are in place to prevent misuse by authorized users?

The ALEISS Security Directive Document Section 11 "Audits and Sanctions for Noncompliance" details processes and procedures in place to minimize misuse and action to be taken when misuse is discovered.

Do other systems share data or interface with data in this system?

ALEISS Consortium Agencies contribute read-only information to ALEISS. Only ALEISS Consortium Agencies share the data housed on the ALEISS node by individual access and query. No automated interface "shares" access to ALEISS data. Knowledge Computing Corporation maintains an interface with the ALEISS node for maintenance and operational support only.

Is data secured in line with Federal Information Security Management Act requirements?

The Federal Information Security Management Act of 2002 governs federal agencies such as the CIA and the Department of Defense. ALEISS is a repository of data from local and state law enforcement only. It includes no data from Federal agencies. Therefore, the specific requirements enumerated in the act do not apply to ALEISS.

ALEISS has in place detailed and specific directives and procedures regarding system and data security. Please refer to the attached supplement.

If system is operated in multiple sites, how will consistent use of system and data be maintained?

System is located at a single secure site, where systems and data will be maintained and secured by staff of the National Law Enforcement and Corrections Technology Center-Northwest (NLECTC-NW).

What are retention periods for data in system?

The data on the ALEISS node is a replica of data in the contributing agency's RMS, therefore the retention period will be determined by the contributing agency procedure and/or applicable laws.

What are the procedures for expunging?

Data on the ALEISS node is a replica of data in the contributing agency's RMS. Decisions for expunging of records will be made by the contributing agency.

Will system allow the monitoring of groups/individuals?

The system features a capability whereby an authorized investigator can ask to be alerted by email if another user runs a query on a given suspect. This is meant as an investigative aid only, because it is common for two investigators to be simultaneously investigating an active criminal. The investigator will be encouraged to contact the source department to verify the data and determine any significance to the current investigation.

What controls exist to prevent unauthorized monitoring?

The ALEISS Security Directive Document Section 11 “Audits and Sanctions for Noncompliance” details processes and procedures in place to identify any misuse and action to be taken when misuse is discovered.