



DELJIS – The Delaware Criminal Justice System Keeping Sensitive Information Protected from Misuse by Authorized Users

Introduction

Delaware was the first US state to implement an integrated Criminal Justice Information System (CJIS) that supports electronic sharing of criminal justice information within the criminal justice community. While the Delaware CJIS has been in existence since 1990, it is constantly changing to meet the needs of system participants - State and local police, the Attorney General's Office, the Public Defender's Office, the Courts, and the Department of Corrections.

CJIS facilitates the electronic sharing of information among all participating agencies. Specifically, case information, from initial contact to case-closing events, is available to CJIS participants. For example, warrant and incarceration information is available to CJIS participants instantly; court dispositions are electronically transmitted to the State Bureau of Identification (SBI); and Protection From Abuse Orders, created on-line in Family Court, are available to all CJIS participants in real-time.

Users are able to determine the status of a case instantly, which greatly enhances the ability to process criminal cases efficiently. Law enforcement's instant access to criminal history, warrant and protection order information has been a critical component of system success. Public safety has been greatly enhanced by the efficient exchange of such background information.

CJIS is based on a central mainframe system which provides several types of user interfaces. These include secured web access to law enforcement officers enabling them to access the system from their patrol cars. Access to CJIS is protected by standard security tools which grant access only to authorized end-users. However, these tools do not monitor how end-users utilize their authorized access and cannot detect or prevent misuse by the authorized end-users.

The Challenges

CJIS serves over 7,000 end-users. Various types of authorized end-users may pose a potential threat:

- A disgruntled employee that has easy access to confidential data
- An employee who is "just looking" and then "telling" something which is protected information
- An employee looking to "harm" another person by disclosing information
- An employee looking for financial gain by selling sensitive information

Various types of data may be leaked:

- Arrest data
- Complaint/ Incident data
- Crime data
- Motor vehicle and license data

As the information maintained by CJIS is highly sensitive there are many cases that require the ability to reconstruct user actions in order to find what specific data was accessed by which user. In addition it is needed to know beyond a "reasonable doubt" that no one else had accessed the same information within the relevant timeframe.

Like other systems, CJIS maintains log files stored on tapes. However, these logs were not intended to be used as an audit trail and are not "easily" human-readable.

"The Intellinx results were overwhelmingly jaw dropping successful. The logging system performed fantastically better than expected. Turnaround time with the Intellinx system was fabulous.

Breach investigation time decreased by more than 90%.

Potential threats to officer and public safety are reduced.

The implementation did not require any changes to our application code and does not impact system performance."



Ms. Peggy Bell

Executive Director,
Delaware Criminal Justice
Information System
(DELJIS),
the State of Delaware

Prior to implementing Intellinx, investigators needed to plow through mountains of paper logs as shown in the picture below. Depending on the type of search requested, one second's activity could be represented by one box full of paper.

The old investigation process had significant shortcomings:

- Labor intensive (pulling and mounting tapes)
- Room for error (missing or damaged tapes)
- Printing and reviewing logs and screens is tedious and prone to errors
- Very long turnaround time for investigations.

For example, reviewing 6 months of data took 2½ months!

As a result, requests for investigating activity logs were honored only for "major crime", not for other suspicious cases.

The Goals in Searching for a New Solution

The Secretary of the Department of Technology and Information and CIO for the State of Delaware, Thomas Jarrett, recognized the critical situation DELJIS was facing and searched for a solution. The desired solution was supposed to meet the following goals:

- Reduce the time associated with investigations
- Have potentially "real time" answers to questions of "Who? Did What? When?"
- Enforce state laws
- Ensure "public and police safety" by reducing the number of threats
- Assist Law Enforcement with criminal investigations of homicides and burglaries
- Provide a log of vehicle or license information that may have been accessed on a recent traffic stop to be used in the search for a missing or wanted person
- Set alerts on names, license, identifying number, case number, complaint number, warrant number to see if anyone accesses this information

The Intellinx Solution

The Intellinx solution was installed for evaluation in late 2006. Within a few hours the system was up and running and started to record the activity of all end-users connected to the mainframe. The system reconstructs end-user sessions and allows investigators to quickly search for user sessions based on any field value that appeared in any user screen. Investigators can now visually replay user sessions, screen by screen. The evaluation installation was very successful and allowed the State to meet its goals. After the contract negotiations were finalized the system was implemented in production environment.

The Intellinx patent-pending technology tracks user behavior patterns at the application screen level and can build profiles of users and user-groups. The Intellinx Analytic Engine generates alerts on suspicious events in real-time. An event may be considered suspicious if the current activity of an end-user is different from his normal behavior in the past or if his behavior is different from his peers in the same department or peers with similar roles.

The Results

The Intellinx solution dramatically reduced the duration of internal investigations by more than 90%. For example, investigating 6 months of data takes 20 minutes using Intellinx, where it took 2½ months previously. It enables DELJIS to investigate every request from law enforcement agencies, not only major crimes as before. For example, in one of the cases an agency requested to check if any user accessed specific warrant information. A quick investigation using Intellinx revealed that a specific user accessed information on this warrant and disseminated it to an unauthorized person. This case resulted in one user arrest, one user terminated, and one user administratively reprimanded and losing access to the system.



Two weeks worth of logs

The Intellinx Benefits

- Deters users just by knowing that all their actions are recorded
- Improves effectiveness by advising of a suspicious behavior
- Provides full visibility to user actions
- Enhances the State's ability to enforce Delaware laws relating to access and dissemination of records
- Real-time Alerts allow enforcing security policies by detecting security breaches immediately and enhancing officer safety
- Recorded data is encrypted and digitally signed which allowed it to be accepted as forensic evidence in court hearings
- Totally non-invasive and does not have any performance impact

As Intellinx encrypts and digitally signs the recorded data, data from the Intellinx system was accepted as forensic evidence in at least one case at a Federal Court and one in a State Court.